aws

Guía del usuario

Amazon Elastic Compute Cloud

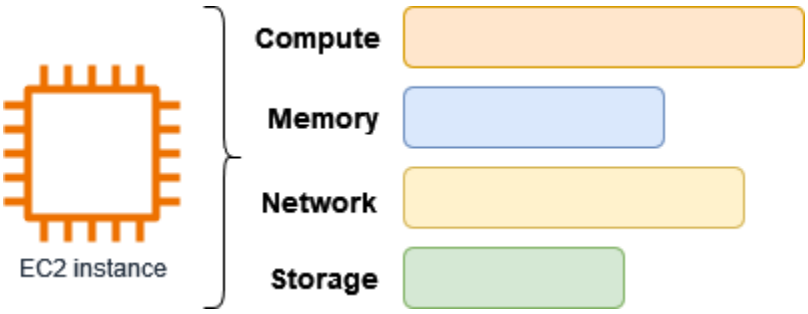
Amazon Elastic Compute Cloud: Guía del usuario

Table of Contents

¿Qué es Amazon EC2?

Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad de computación escalable bajo demanda en la nube de Amazon Web Services (AWS). El uso de Amazon EC2 reduce los costos de hardware para que pueda desarrollar e implementar aplicaciones con mayor rapidez. Puede usar Amazon EC2 para lanzar tantos servidores virtuales como necesite, configurar la seguridad y las redes, y administrar el almacenamiento. Puede agregar capacidad (escalar verticalmente) para gestionar tareas que requieren mucha computación, como los procesos mensuales o anuales, o los picos de tráfico del sitio web. Cuando el uso disminuye, puede volver a reducir la capacidad (reducir verticalmente).

Una instancia de EC2 es un servidor virtual en la nube de AWS. Cuando inicia una instancia de EC2, el tipo de instancia que especifica determina el hardware disponible para la instancia. Cada tipo de instancia ofrece una combinación diferente de recursos de computación, memoria, red y almacenamiento. Para obtener más información, consulte la Guía de tipos de instancia de Amazon EC2.



Características de Amazon EC2

Amazon EC2 ofrece las siguientes características de nivel alto:

instancias

Servidores virtuales.

Imágenes de máquina de Amazon (AMI)

Plantillas preconfiguradas para las instancias que empaquetan los componentes que necesita para el servidor (incluido el sistema operativo y el software adicional).

Tipos de instancias

Varias configuraciones de CPU, memoria, almacenamiento, capacidad de red y gráficos para las instancias.

Volúmenes de Amazon EBS

Volúmenes de almacenamiento persistente para los datos mediante Amazon Elastic Block Store (Amazon EBS).

Volúmenes de almacén de instancias

Volúmenes de almacenamiento para datos temporales que se eliminan cuando una instancia se detiene, se termina o se pone en hibernación.

Pares de claves

Información de inicio de sesión segura para las instancias. AWS almacena la clave pública y usted guarda la clave privada en un lugar seguro.

Grupos de seguridad

Un firewall virtual que le permite especificar los protocolos, los puertos y los rangos de IP de origen que pueden llegar a sus instancias, y los rangos de IP de destino a los que se pueden conectar las instancias.

Amazon EC2 admite el procesamiento, el almacenamiento y la transmisión de datos de tarjetas de crédito por parte de un comerciante o un proveedor de servicios y se ha validado por estar conforme con el Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI DSS). Para obtener más información acerca de PCI DSS, incluido cómo solicitar una copia del Paquete de conformidad con PCI de AWS, consulte PCI DSS Nivel 1.

Servicios relacionados

Servicios para utilizar con Amazon EC2

Puede usar otros Servicios de AWS con las instancias que implemente mediante Amazon EC2.

Amazon EC2 Auto Scaling

Le ayuda a garantizar que cuenta con la cantidad correcta de instancias de Amazon EC2 disponibles para controlar la carga de su aplicación.

AWS Backup

Automatice las copias de seguridad de sus instancias de Amazon EC2 y de los volúmenes de Amazon EBS adjuntos a ellas.

Amazon CloudWatch

Supervise sus instancias y volúmenes de Amazon EBS.

Elastic Load Balancing

Distribuya automáticamente el tráfico de entrada de aplicaciones entre múltiples instancias.

Amazon GuardDuty

Detecte el uso potencialmente no autorizado o malintencionado de sus instancias de EC2.

EC2 Image Builder

Automatice la creación, la administración y la implementación de imágenes de servidor personalizadas, seguras y actualizadas.

AWS Launch Wizard

Dimensione, configure e implemente recursos de AWS para aplicaciones de terceros sin tener que identificar ni aprovisionar manualmente los recursos de AWS individuales.

AWS Systems Manager

Realice operaciones a escala en instancias EC2 con esta solución de administración segura e integral.

Servicios de computación adicionales

Puede lanzar instancias mediante otro servicio de computación de AWS en lugar de utilizar Amazon EC2.

Amazon Lightsail

Cree sitios web o aplicaciones web con Amazon Lightsail, una plataforma en la nube que proporciona los recursos que necesita para implementar su proyecto rápidamente, por un precio mensual bajo y predecible. Para comparar Amazon EC2 y Lightsail, consulte Amazon Lightsail o Amazon EC2.

Amazon Elastic Container Service (Amazon ECS)

Implemente, administre y escale aplicaciones en contenedores en un clúster de instancias de EC2. Para obtener más información, consulte Cómo elegir un servicio de contenedor de AWS.

Amazon Elastic Kubernetes Service (Amazon EKS)

Ejecute sus aplicaciones de Kubernetes en AWS. Para obtener más información, consulte Cómo elegir un servicio de contenedor de AWS.

Acceder a Amazon EC2

Puede crear y administrar las instancias de Amazon EC2 con cualquiera de las siguientes interfaces:

Consola de Amazon EC2

Una interfaz web sencilla para crear y administrar instancias y recursos de Amazon EC2. Si se ha inscrito en una cuenta de AWS, podrá obtener acceso a la consola de Amazon EC2 iniciando sesión en la AWS Management Console y seleccionando EC2 en la página de inicio.

AWS Command Line Interface

Le permite interactuar con los servicios de AWS mediante el uso de comandos en el intérprete de comandos de la línea de comandos. Es compatible con Windows, Mac y Linux. Para obtener más información sobre la AWS CLI, consulte la Guía del usuario de AWS Command Line Interface. Puede encontrar los comandos de Amazon EC2 en la Referencia de comandos de AWS CLI.

AWS CloudFormation

Amazon EC2 admite la creación de recursos utilizando AWS CloudFormation. Cree una plantilla, en formato JSON o YAML, que describa sus recursos de AWS para que AWS CloudFormation aprovisione y configure esos recursos en su nombre. Puede reutilizar las plantillas de CloudFormation para aprovisionar los mismos recursos varias veces, ya sea en la misma región y cuenta o en varias regiones y cuentas. Para obtener más información acerca de los tipos de recursos y las propiedades de Amazon EC2 compatibles, consulte Referencia de tipos de recursos de EC2 en la Guía del usuario de AWS CloudFormation.

SDK de AWS

Si prefiere crear aplicaciones usando API específicas de un lenguaje en lugar de enviar una solicitud a través de HTTP o HTTPS, AWS le proporciona bibliotecas, ejemplos de código, tutoriales y otros recursos para desarrolladores de software. Estas bibliotecas proporcionan

funciones básicas que automatizan tareas como la firma criptográfica de las solicitudes o el tratamiento de las respuestas de error, facilitándole así el comienzo. Para obtener más información, consulte Herramientas para crear en AWS.

AWS Tools for PowerShell

Un conjunto de módulos de PowerShell basados en la funcionalidad expuesta en AWS SDK for .NET. Las herramientas para PowerShell le permiten llevar a cabo operaciones mediante script en sus recursos de AWS desde la línea de comandos de PowerShell. Para empezar, consulte la AWS Tools for Windows PowerShell Guía del usuario de . Puede encontrar los cmdlets para Amazon EC2 en la Referencia de cmdlets de AWS Tools for PowerShell.

API de consulta

Amazon EC2 ofrece un API de consulta. Estas solicitudes son solicitudes de HTTP o HTTPS que utilizan los verbos GET o POST de HTTP y un parámetro de consulta denominado `Action`. Para obtener más información acerca de las acciones de la API para Amazon EC2, consulte Acciones en la Amazon EC2 API Reference.

Precios de las Amazon EC2

Amazon EC2 ofrece las siguientes opciones de precios:

Capa gratuita

Puede comenzar con Amazon EC2 de manera gratuita. Para explorar las opciones del nivel gratuito, consulta Nivel gratuito de AWS.

instancias bajo demanda

Pague por las instancias que utiliza por segundo, con un mínimo de 60 segundos, sin compromisos a largo plazo ni pagos iniciales.

Savings Plans

Puede reducir los costos de Amazon EC2 comprometiéndose a una cantidad de uso constante, en USD por hora, durante un período de 1 o 3 años.

Reserved Instances

Puede reducir sus costos de Amazon EC2 comprometiéndose con una configuración de instancia específica, incluido el tipo de instancia y la región, por un período de 1 o 3 años.

Spot Instances

Solicite instancias EC2 no utilizadas, que pueden reducir sus costos de Amazon EC2 considerablemente.

Hosts dedicados

Reduzca los costos mediante el uso de un servidor de EC2 físico totalmente dedicado a su uso, ya sea bajo demanda o como parte de Savings Plans. Puede utilizar sus licencias de software vinculadas a servidores existentes y obtener ayuda para cumplir con los requisitos de cumplimiento.

Reservas de capacidad bajo demanda

Reserve capacidad de computación para las instancias de EC2 en una zona de disponibilidad específica para cualquier duración.

Facturación por segundo

Elimina el costo de los minutos y segundos no utilizados de la factura.

Para obtener una lista completa de los costos y precios de Amazon EC2 y más información sobre los modelos de compra, consulte Precios de Amazon EC2.

Estimaciones, facturación y optimización de costos

Para crear estimaciones para sus casos de uso de AWS, utilice AWS Pricing Calculator.

Para calcular el costo de transformar cargas de trabajo de Microsoft en una arquitectura moderna que utilice servicios de código abierto y nativos en la nube implementados en AWS, utilice la Calculadora de modernización de AWS para cargas de trabajo de Microsoft.

Para ver su factura, vaya al Panel de Billing and Cost Management en la consola de AWS Billing and Cost Management. La factura contiene vínculos a informes de uso que ofrecen detalles sobre la cuenta. Para obtener más información sobre la facturación de la cuenta de AWS, consulte la Guía del usuario de facturación y administración de costes de AWS.

Si tiene alguna pregunta sobre los eventos, las cuentas y la facturación de AWS, póngase en contacto con AWS Support.

Para calcular el costo de un entorno aprovisionado de ejemplo, consulte Centro de ahorro de la nube.. Al calcular el costo de un entorno aprovisionado, recuerde incluir los costos incidentales, como el almacenamiento de instantáneas para volúmenes de EBS.

Puede optimizar el costo, la seguridad y el rendimiento de su entorno de AWS con AWS Trusted Advisor.

Puede utilizar AWS Cost Explorer para analizar el costo y el uso de las instancias EC2. Puede ver los datos de los últimos 13 meses y predecir la cantidad que probablemente va a gastar durante los 12 meses siguientes. Para obtener más información, consulte Análisis de los costos con AWS Cost Explorer en la Guía del usuario de AWS Cost Management.

Recursos

- Características de Amazon EC2
- AWS re:Post
- Skill Builder de AWS
- Soporte de AWS
- Tutoriales prácticos
- Alojamiento web
- Windows en AWS

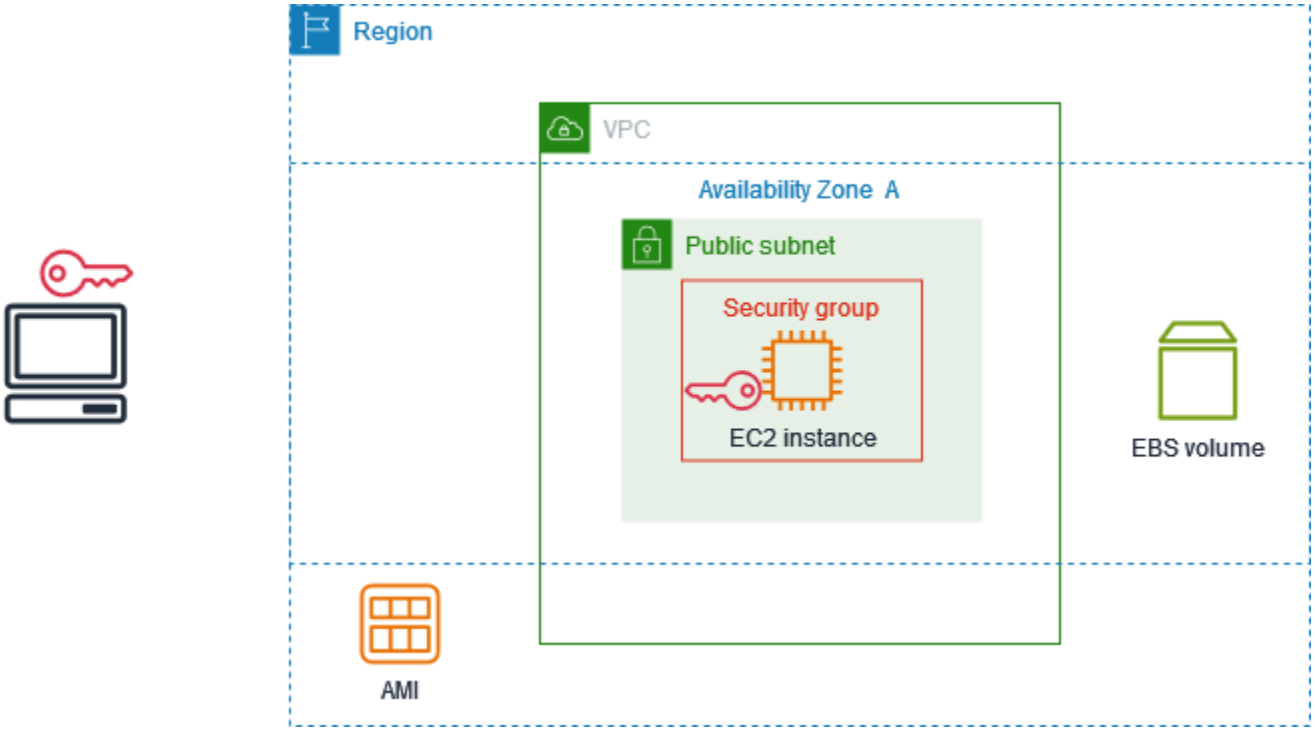
Introducción a Amazon EC2

Utilice esta explicación para empezar con Amazon Elastic Compute Cloud (Amazon EC2). Aprenderá a lanzar y conectarse a una instancia EC2. Una instancia es un servidor virtual en la nube de AWS. Con Amazon EC2, puede instalar y configurar el sistema operativo y las aplicaciones que se ejecutan en la instancia.

Información general

En el siguiente diagrama se muestran los componentes clave que se utilizan en este tutorial:

- Una imagen: plantilla que contiene el software que se va a ejecutar en la instancia, como el sistema operativo.
- Un par de claves: es un conjunto de credenciales de seguridad que se usa para demostrar la identidad al conectarse a una instancia . Se almacena una clave privada en el equipo y una clave pública en la instancia.
- Una red: una nube privada virtual (VPC) es una red virtual dedicada para su Cuenta de AWS. Para ayudarlo a comenzar rápidamente, su cuenta incluye una VPC predeterminada en cada Región de AWS, y cada VPC predeterminada tiene una subred predeterminada en cada zona de disponibilidad.
- Un grupo de seguridad: funciona como un firewall virtual para controlar el tráfico entrante y saliente.
- Un volumen de EBS: necesitamos un volumen raíz para la imagen. Si lo desea, puede agregar volúmenes de datos.



Costo de este tutorial

Cuando se registra en AWS, puede comenzar a usar Amazon EC2 mediante el capa gratuita de AWS. Si creó la Cuenta de AWS hace menos de 12 meses y aún no ha excedido los beneficios del nivel gratuito para Amazon EC2, no incurrirá en costos para completar este tutorial, porque lo ayudamos a seleccionar opciones que estén dentro de los beneficios del nivel gratuito. En otro caso, incurrirá en los costos de uso estándar de Amazon EC2 desde el momento en que lance la instancia hasta que la termine (que es la tarea final de este tutorial), incluso si permanece inactiva.

Si desea obtener instrucciones para determinar si es elegible para el nivel gratuito, consulte the section called “Seguimiento del uso del nivel gratuito”.

Tareas

- Paso 1: lance una instancia
- Paso 2: Conexión a la instancia
- Paso 3: Eliminación de la instancia
- Siguientes pasos

Paso 1: lance una instancia

Puede lanzar una instancia EC2 mediante la AWS Management Console, tal como se describe en el siguiente procedimiento. Este tutorial tiene por objetivo ayudarlo a lanzar su primera instancia dentro de los beneficios del nivel gratuito rápidamente, por lo que no cubre todas las opciones posibles.

Para lanzar una instancia

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la barra de navegación de la parte superior de la pantalla, se muestra la Región de AWS actual (por ejemplo, Ohio). Puede usar la región seleccionada o, si lo desea, seleccionar una región que esté más cerca de usted.
3. En el panel de la consola de EC2, en el panel Iniciar instancia, elija Iniciar instancia.
4. En Name and tags (Nombre y etiquetas), ingrese un nombre descriptivo para la instancia en Name (Name).
5. En Application and OS Images (Amazon Machine Image) (Imágenes de aplicaciones y sistema operativo [imagen de máquina de Amazon]), realice lo siguiente:
   a. Elija Inicio rápido y elija el sistema operativo (SO) de la instancia. Para la primera instancia de Linux, le recomendamos que elija Amazon Linux.
   b. En Imagen de máquina de Amazon (AMI), seleccione una AMI que esté marcada como apta para el nivel gratuito.
6. En Tipo de instancia, para Tipo de instancia, elija `t2.micro`, que cumpla los requisitos para el nivel gratuito. En las regiones en las que `t2.micro` no está disponible, `t3.micro` es apto para el nivel gratuito.
7. En Par de claves (inicio de sesión), para Nombre del par de claves, seleccione un par de claves existente o elija Crear nuevo par de claves para crear el primero.

   > **Warning**
   >
   > Si elige Continuar sin un par de claves (no recomendado), no podrá conectarse a la instancia mediante los métodos que se describen en este tutorial.

8. En Configuración de red, observe que seleccionamos su VPC predeterminada y la opción de usar la subred predeterminada en una zona de disponibilidad que elijamos para usted, y configuramos un grupo de seguridad con una regla que permite las conexiones a su instancia

desde cualquier lugar. Para la primera instancia, le recomendamos que utilice la configuración predeterminada. De lo contrario, puede actualizar la configuración de red de la siguiente manera:

- (Opcional) Para usar una subred predeterminada específica, seleccione Editar y, a continuación, elija una subred.
- (Opcional) Para usar una VPC diferente, elija Editar y, a continuación, elija una VPC existente. Si la VPC no está configurada para el acceso público a Internet, no podrá conectarse a la instancia.
- (Opcional) Para restringir el tráfico de conexión entrante a una red específica, seleccione Personalizado en lugar de Cualquier lugar e introduzca el bloque CIDR de su red.
- (Opcional) Para utilizar un grupo de seguridad diferente, elija Seleccionar un grupo de seguridad existente y, a continuación, elija un grupo de seguridad existente. Si el grupo de seguridad no tiene una regla que permita el tráfico de conexión desde la red, no podrá conectarse a la instancia. En el caso de una instancia de Linux, debe permitir el tráfico SSH. En el caso de una instancia de Windows, debe permitir el tráfico RDP.

9. En Configurar almacenamiento, observe que configuramos un volumen raíz, pero no un volumen de datos. Esto es suficiente para fines de prueba.
10. Revise un resumen de la configuración de su instancia en el panel Summary (Resumen); cuando haya terminado, elija Launch instance.
11. Si el lanzamiento se ha realizado correctamente, elija el ID de la instancia en la notificación de Éxito para abrir la página Instancias y supervisar el estado del lanzamiento.
12. Seleccione la casilla de verificación de la instancia. El estado inicial de una instancia es `pending`. Una vez iniciada la instancia, su estado cambia a `running`. Seleccione la pestaña Estado y alarmas. Una vez que la instancia pase las comprobaciones de estado, estará lista para recibir solicitudes de conexión.

Paso 2: Conexión a la instancia

El procedimiento que utiliza depende del sistema operativo de la instancia. Si no puede conectarse a la instancia, consulte Solución de problemas de conexión a la instancia de Linux para obtener asistencia.

instancias de Linux

Puede conectarse a la instancia de Linux mediante un cliente SSH. Si está ejecutando Windows en su equipo, abra un terminal y ejecute el comando `ssh` para comprobar que tiene un cliente SSH instalado. Si no encuentra el comando, instale OpenSSH para Windows.

Para conectarse a la instancia mediante SSH

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Seleccione la instancia y, a continuación, elija Connect (Conectar).
4. En la página Conectarse a la instancia, elija la pestaña Cliente SSH.
5. (Opcional) Si creó un par de claves al lanzar la instancia y descargó la clave privada (archivo .pem) en un equipo con Linux o macOS, ejecute el comando chmod de ejemplo para configurar los permisos de la clave privada.
6. Copie el comando SSH de ejemplo. A continuación se muestra un ejemplo en el que *key-pair-name*.pem es el nombre del archivo de clave privada, *ec2-user* es el nombre de usuario asociado a la imagen y la cadena que sigue al símbolo @ es el nombre de DNS público de la instancia.

   ```
   ssh -i key-pair-name.pem ec2-user@ec2-198-51-100-1.us-east-2.compute.amazonaws.com
   ```

7. En una ventana del terminal de su equipo, ejecute el comando ssh que guardó en el paso anterior. Si el archivo de clave privada no está en el directorio actual, debe especificar la ruta completa al archivo de clave en este comando.

   A continuación, se muestra un ejemplo de respuesta:

   ```
   The authenticity of host 'ec2-198-51-100-1.us-east-2.compute.amazonaws.com
    (198-51-100-1)' can't be established.
   ECDSA key fingerprint is l4UB/neBad9tvkgJf1QZWxheQmR59WgrgzEimCG6kZY.
   Are you sure you want to continue connecting (yes/no)?
   ```

8. (Opcional) Verifique que la huella digital en la alerta de seguridad coincida con la huella digital de la instancia que aparece en la salida de la consola cuando inicia una instancia por primera vez. Para obtener el resultado de la consola, seleccione Acciones, Supervisar y solucionar problemas, Obtener el registro del sistema. Si las huellas digitales no coinciden, alguien podría intentar un ataque de intermediario. Si coinciden, continúe con el siguiente paso.

9. Escriba **`yes`**.

   A continuación, se muestra un ejemplo de respuesta:

```
Warning: Permanently added 'ec2-198-51-100-1.us-
east-2.compute.amazonaws.com' (ECDSA) to the list of known hosts.
```

instancias de Windows

Para conectarse a una instancia de Windows, deber recuperar la contraseña inicial de administrador y usar esta contraseña cuando se conecte a la instancia mediante el escritorio remoto. Pasarán unos minutos desde que la instancia se inicia hasta que la contraseña está disponible.

El nombre de usuario predeterminado de la cuenta de administrador depende del idioma del sistema operativo (SO) incluido en la AMI. Para determinar el nombre de usuario correcto, identifique el idioma del sistema operativo de la AMI y, a continuación, elija el nombre de usuario correspondiente. Por ejemplo, en el caso de un sistema operativo en inglés, el nombre de usuario es `Administrator`; en el caso de un sistema operativo en francés, es `Administrateur`; y en el caso de un sistema operativo en portugués, es `Administrador`. Si la versión de un idioma del sistema operativo no tiene un nombre de usuario en el mismo idioma, elija el nombre de usuario `Administrator (Other)`. Para obtener más información, consulte Localized Names for Administrator Account in Windows en el Wiki de Microsoft TechNet.

Si ha unido su instancia a un dominio, puede conectarse a la instancia con las credenciales de dominio que haya definido en AWS Directory Service. En la pantalla de inicio de sesión del escritorio remoto, en lugar de utilizar el nombre del ordenador local y la contraseña generada, utilice el nombre de usuario completo para el administrador (por ejemplo, **`corp.example.com\Admin`**) y la contraseña de esta cuenta.

Si aparece un error al intentar conectarse a la instancia, consulte the section called “El escritorio remoto no puede conectarse al equipo remoto”.

Para conectarse a la instancia de Windows mediante un cliente RDP

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Seleccione la instancia y, a continuación, elija Connect (Conectar).
4. En la página Conectarse a la instancia, elija la pestaña Cliente de RDP.

5. En Nombre de usuario, elija el nombre de usuario predeterminado de la cuenta de administrador. El nombre de usuario que elija debe coincidir con el idioma del sistema operativo (SO) incluido en la AMI que utilizó para iniciar la instancia. Si no hay ningún nombre de usuario en el mismo idioma que su sistema operativo, elija Administrador (otro).
6. Elija Obtener contraseña.
7. En la página Obtener contraseña de Windows, haga lo siguiente:
   a. Elija Cargar archivo de clave privada y vaya el archivo de clave privada (`.pem`) que especificó al iniciar la instancia. Seleccione el archivo y elija Open (Abrir) para copiar todo el contenido del archivo en esta ventana.
   b. Elija Descifrar contraseña. La página Obtener contraseña de Windows se cierra y la contraseña de administrador predeterminada de la instancia aparece en Contraseña y reemplaza al enlace Obtener contraseña mostrado anteriormente.
   c. Copie la contraseña y guárdela en un lugar seguro. Necesitará la contraseña para conectarse a la instancia.
8. Elija Download remote desktop file (Descargar archivo de escritorio remoto). Cuando haya terminado de descargar el archivo, elija Cancel (Cancelar) para volver a la página Instances (instancia[s]). Desplácese hasta el directorio de descargas y abra el archivo RDP.
9. Es posible que aparezca una advertencia en la que se indique que se desconoce el publicador de la conexión remota. Elija Connect (Conectarse) para conectarse a su instancia.
10. La cuenta de administrador está seleccionada de forma predeterminada. Pegue la contraseña que copió anteriormente y, a continuación, elija OK.
11. Debido a la naturaleza de los certificados autofirmados, es posible que aparezca una advertencia que indica que no se pudo autenticar el certificado de seguridad. Realice una de las siguientes acciones siguientes:
    - Si confía en el certificado, seleccione Sí para conectarse a la instancia.
    - [Windows] Antes de continuar, compare la huella digital del certificado con el valor del registro del sistema para confirmar la identidad del equipo remoto. Elija Ver el certificado y, a continuación, seleccione Huella digital en la pestaña Detalles. Compare este valor con el valor de `RDPCERTIFICATE-THUMBPRINT` en Acciones, Supervisar y solucionar problemas, Obtener el registro del sistema.
    - [Mac OS X] Antes de continuar, compare la huella digital del certificado con el valor del registro del sistema para confirmar la identidad del equipo remoto. Seleccione Mostrar certificado, expanda Detalles y elija Huellas digitales SHA1. Compare este valor con el

valor de `RDPCERTIFICATE-THUMBPRINT` en Acciones, Supervisar y solucionar problemas, Obtener el registro del sistema.

Paso 3: Eliminación de la instancia

Cuando haya acabado con la instancia que creó para este tutorial, debería eliminarla terminando la instancia. Si quiere hacer más cosas con esta instancia antes de eliminarla, consulte Siguientes pasos.

> **Important**
>
> Cuando se finaliza una instancia, se elimina totalmente: no es posible volver a conectarse a ella.

Si lanzó una instancia que no está dentro del capa gratuita de AWS, dejará de incurrir en gastos para dicha instancia en cuanto su estado cambie a `shutting down` o `terminated`. Si desea conservar la instancia para más adelante pero no incurrir en ningún gasto, puede detener la instancia ahora y volver a iniciarla más tarde. Para obtener más información, consulte Detención e iniciación de una instancia de Amazon EC2.

Para terminar la instancia

1. En el panel de navegación, seleccione Instances (Instancias). En la lista de instancias, seleccione la instancia.
2. Elija Instance state (Estado de la instancia) y Terminate instance (Terminar instancia).
3. Cuando se le indique que confirme, elija Terminate (Terminar).

   Amazon EC2 apaga y termina la instancia. Una vez terminada la instancia, permanecerá visible en la consola durante un breve periodo y, a continuación, se elimina automáticamente la entrada. No puede quitar la instancia terminada de la pantalla de la consola por sí mismo.

Siguientes pasos

Después de iniciar la instancia, es posible que desee explorar alguno de los siguientes pasos:

- Aprenda cómo hacer un seguimiento del uso del nivel gratuito para evitar sorpresas en la facturación. Para obtener más información, consulte the section called “Seguimiento del uso del nivel gratuito”.
- Configure una alarma CloudWatch para notificarle si el uso excede la capa gratuita. Para obtener más información, consulte Seguimiento del uso del nivel gratuito de AWS en la Guía del usuario de AWS Billing.
- Añada un volumen de EBS. Para obtener más información, consulte Creación de un volumen de Amazon EBS en la Guía del usuario de Amazon EBS.
- Obtenga información sobre cómo administrar de forma remota la instancia de EC2 con el comando Run. Para obtener más información, consulte Run Command de AWS Systems Manager en la Guía del usuario de AWS Systems Manager.
- Obtenga más información sobre las opciones de compra de instancias. Para obtener más información, consulte Opciones de compra de instancias.
- Obtenga asesoramiento sobre los tipos de instancias. Para obtener más información, consulte Obtención de recomendaciones de tipos de instancias para una nueva carga de trabajo.

Prácticas recomendadas de Amazon EC2

Se recomienda realizar las siguientes prácticas recomendadas si desea aprovechar al máximo los beneficios de Amazon EC2.

Seguridad

- Administre el acceso a las API y a los recursos de AWS con la federación de identidades y los roles de IAM. Para obtener más información, consulte Creación de políticas de IAM en la Guía del usuario de IAM.
- Implemente las reglas menos permisivas en su grupo de seguridad. Para obtener más información, consulte Reglas del grupo de seguridad.
- Corrija, actualice y proteja con regularidad el sistema operativo y las aplicaciones de su instancia. Para obtener más información, consulte Administración de actualizaciones. Para obtener instrucciones específicas para los sistemas operativos Windows, consulte Prácticas recomendadas de seguridad para instancias de Windows.
- Utilice Amazon Inspector para detectar y analizar las instancias de Amazon EC2 de forma automática en busca de vulnerabilidades de software y exposición no deseada en la red. Para obtener más información, consulte la Guía del usuario de Amazon Inspector.
- Utilice controles de AWS Security Hub para supervisar sus recursos de Amazon EC2 comparándolos con las mejores prácticas de seguridad y los estándares de seguridad. Para obtener más información sobre los grupos de seguridad, consulte Amazon Elastic Compute Cloud controls (Controles de Amazon Elastic Compute Cloud) en la Guía del usuario de AWS Security Hub.

Almacenamiento

- Entienda las implicaciones del tipo de dispositivo raíz para la persistencia, el backup y la recuperación de los datos. Para obtener más información, consulte Almacenamiento para el dispositivo raíz.
- Utilice volúmenes de Amazon EBS diferentes para los sistemas operativos y los datos. Compruebe que el volumen que tiene sus datos persista después de la terminación de la instancia. Para obtener más información, consulte Conservación de los datos cuando se termina una instancia.
- Utilice el almacén de instancias disponible para su instancia para almacenar datos temporales. Recuerde que los datos almacenados en un almacén de instancias se eliminan cuando una

instancia se detiene, se termina o se pone en hibernación. Si utiliza el almacén de instancias para el almacenamiento de la base de datos, asegúrese de tener un clúster con un factor de replicación que asegure la tolerancia a errores.

- Cifrar volúmenes e instantáneas de EBS. Para obtener más información, consulte Cifrado de Amazon EBS en la Guía del usuario de Amazon EBS.

Administración de recursos

- Utilice los metadatos de las instancias y las etiquetas de recursos personalizadas para realizar el seguimiento de sus recursos de AWS e identificarlos. Para obtener más información, consulte Trabajar con metadatos de instancias y Etiquetar los recursos de Amazon EC2.
- Visualice sus límites actuales para Amazon EC2. Planifique la solicitud del aumento de los límites antes del momento en que lo necesite. Para obtener más información, consulte Cuotas de servicio de Amazon EC2.
- Utilice AWS Trusted Advisor para inspeccionar el entorno de AWS y, a continuación, realice recomendaciones cuando surja la oportunidad de ahorrar dinero, mejorar el rendimiento y la disponibilidad del sistema o ayudar a cerrar las brechas de seguridad. Para obtener más información, consulte AWS Trusted Advisor en la Guía del usuario de AWS Support.

Copia de seguridad y recuperación

- Haga con regularidad una copia de seguridad de sus volúmenes de EBS utilizando instantáneas de Amazon EBS y creando una Amazon Machine Image (AMI) a partir de la instancia para guardar la configuración como una plantilla para lanzar instancias en el futuro. Para obtener más información acerca de los servicios de AWS que ayudan a lograr este caso de uso, consulte AWS Backup y Amazon Data Lifecycle Manager.
- Implemente componentes fundamentales de su aplicación en varias zonas de disponibilidad y replique sus datos de forma adecuada.
- Diseñe sus aplicaciones para que gestionen las direcciones IP dinámicas cuando su instancia se reinicie. Para obtener más información, consulte Direccionamiento IP de instancias Amazon EC2.
- Supervise los eventos y responda a ellos. Para obtener más información, consulte Monitorear Amazon EC2.
- Compruebe que esté preparado para gestionar una conmutación por error. En una solución básica, puede conectar manualmente una interfaz de red o una dirección IP elástica a una instancia de sustitución. Para obtener más información, consulte Interfaces de red elásticas. En una solución

automática, puede utilizar Amazon EC2 Auto Scaling. Para obtener más información, consulte la Guía del usuario de Amazon EC2 Auto Scaling.

- Pruebe periódicamente el proceso de recuperación de las instancias y los volúmenes de Amazon EBS a fin de garantizar que los datos y los servicios se restauren correctamente.

Redes

- Establezca el valor de tiempo de vida (TTL) para las aplicaciones en 255, para IPv4 e IPv6. Si utiliza un valor menor, existe el riesgo de que el TTL caduque mientras el tráfico de la aplicación está en tránsito, lo que provoca problemas de accesibilidad para las instancias.

Imágenes de máquina de Amazon (AMI)

Una imagen de máquina de Amazon (AMI) es una imagen compatible y mantenida que ofrece AWS y que brinda la información necesaria para iniciar una instancia. Debe especificar una AMI al iniciar una instancia. Cuando necesite varias instancias con la misma configuración, puede iniciarlas desde una misma AMI. Cuando necesite instancias con distintas configuraciones, puede utilizar distintas AMI para iniciarlas.

Una AMI incluye lo siguiente:

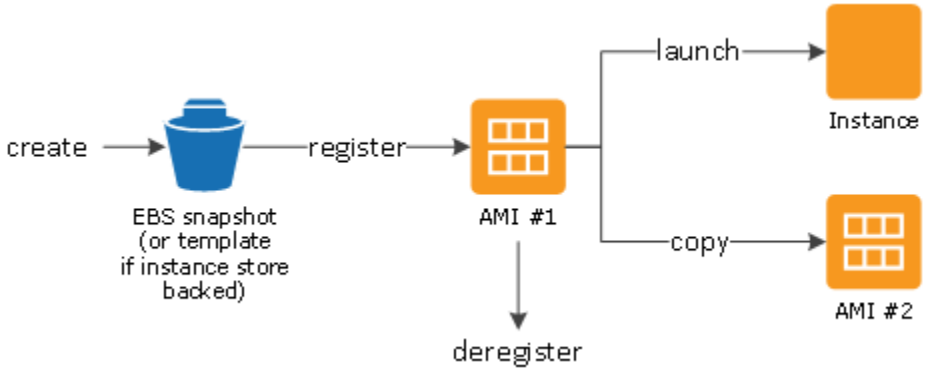
- Una o más instantáneas de Amazon Elastic Block Store (Amazon EBS) o, para las AMI con respaldo en el almacenamiento de la instancia, una plantilla para el volumen raíz de la instancia (por ejemplo, un sistema operativo, un servidor de aplicaciones y aplicaciones).
- Permisos de inicialización que controlan qué cuentas de AWS pueden utilizar la AMI para iniciar instancias.
- Un asignación de dispositivos de bloques que especifica los volúmenes que se van a adjuntar a la instancia cuando se inicialice.

Temas sobre la imagen de máquina de Amazon (AMI)

- Supervisión de los eventos de las AMI con Amazon EventBridge
- Comprender la información de facturación de la AMI
- Cuotas de IAM

Usar una AMI

En el siguiente diagrama, se resume el ciclo de vida de la AMI. Después de crear y registrar una AMI, puede utilizarla para iniciar nuevas instancias. (También puede iniciar instancias desde una AMI si el propietario de la AMI concede permisos de inicialización). Puede copiar una AMI dentro de la misma región de AWS o en regiones de AWS diferentes. Cuando ya no necesite una AMI, puede cancelar su registro.



Puede buscar una AMI que cumpla los criterios de su instancia. Puede buscar las AMI que proporciona AWS o las AMI que proporciona la comunidad. Para obtener más información, consulte Tipos de AMI y Buscar una AMI.

Después de iniciar la instancia desde una AMI, puede conectarse a ella. Si está conectado a una instancia, puede usarla como cualquier otro servidor. Para obtener información acerca de la inicialización, la conexión y el uso de la instancia, consulte Introducción a Amazon EC2.

Crear su propia AMI

Puede lanzar una instancia desde una AMI existente, personalizar la instancia (como, por ejemplo, instalar un software en la instancia) y luego guardar la configuración actualizada como una AMI personalizada. Las instancias que se lancen desde la nueva AMI personalizada incluirán todas las configuraciones que definió al crearla.

El dispositivo de almacenamiento raíz de la instancia determina el proceso que se sigue para crear una AMI. El volumen raíz de una instancia es un volumen de Amazon Elastic Block Store (Amazon

EBS) o un volumen de almacenes de instancias. Para obtener más información acerca de los volúmenes de dispositivo raíz, consulte Volumen raíz de la instancia de Amazon EC2.

- Para crear una AMI con respaldo de Amazon EBS, consulte Creación de una AMI basada en Amazon EBS.
- Para crear una AMI con respaldo en el almacenamiento de la instancia, consulte Crear una AMI de Linux con respaldo en el almacén de instancias.

Para facilitar la clasificación y la administración de las AMI, puede asignarles etiquetas personalizadas. Para obtener más información, consulte Etiquetar los recursos de Amazon EC2.

Comprar, compartir y vender AMI

Después de crear una AMI, puede mantenerla en privado para que solo pueda usarla usted o puede compartirla con una lista especificada de cuentas de AWS. También puede hacer pública su AMI personalizada para que la comunidad pueda utilizarla. La creación de una AMI segura y útil para el consumo público es un proceso bastante sencillo si se siguen unas directrices muy simples. Para obtener información acerca de cómo crear y utilizar AMI compartidas, consulte AMI compartidas.

Puede adquirir AMI a un tercero, como las AMI que se incluyen en los contratos de servicio de organizaciones como Red Hat. También puede crear una AMI y venderla a otros usuarios de Amazon EC2. Para obtener más información acerca de la compra o venta de AMI, consulte AMI de pago.

Anular el registro de la AMI

Puede anular el registro de una AMI cuando haya terminado con ella. Después de anular el registro de una AMI, no se puede utilizar para iniciar nuevas instancias. Las instancias iniciadas desde la AMI no se verán afectadas. Para obtener más información, consulte Anular el registro de (eliminar) una AMI.

Amazon Linux 2023 y Amazon Linux 2

La última versión de Amazon Linux, AL2023, está optimizada para Amazon EC2 y se proporciona sin costo adicional a los usuarios de Amazon EC2. Las características de AL2023 incluyen una cadencia de inicialización predecible, actualizaciones frecuentes y soporte a largo plazo.

Para obtener más información sobre las características de AL2023 y la inicialización de una AMI de AL2023, consulte:

- Características de AL2023
- Introducción a AL2023

Amazon Linux 2 (AL2) ofrece un entorno de ejecución estable, seguro y de alto rendimiento para las aplicaciones que se ejecutan en Amazon EC2. Para obtener más información, consulte Amazon Linux 2 on Amazon EC2 en la Guía del usuario de Amazon Linux 2.

> **Note**
>
> La AMI de Amazon Linux llegó al final de su vida útil el 31 de diciembre de 2023 y no recibirá actualizaciones de seguridad ni correcciones de errores a partir del 1 de enero de 2024. Para obtener más información sobre el fin de la vida útil de la AMI de Amazon Linux y el soporte de mantenimiento, consulte la publicación de blog Update on Amazon Linux AMI end-of-life. Le recomendamos que actualice las aplicaciones a la versión AL2023, que incluye soporte a largo plazo hasta 2028.

AMI de Windows

AWS proporciona un conjunto de AMI públicamente disponible, que contiene configuraciones de software específicas de la plataforma Windows. Con estas AMI, puede comenzar a crear e implementar rápidamente sus aplicaciones con Amazon EC2. En primer lugar, elija una AMI que cumpla sus requisitos específicos y luego lance una instancia utilizando esa AMI. Recupere la contraseña de la cuenta de administrador y luego inicie sesión en la instancia utilizando Conexión a Escritorio remoto, como en cualquier otro servidor de Windows. Para obtener más información acerca de las AMI de AWS de Windows, consulte la referencia de las AMI de AWS Windows.

Cuando inicia una instancia desde una AMI de Windows, el dispositivo raíz de la instancia de Windows es un volumen de Amazon Elastic Block Store (Amazon EBS). Las AMI de Windows no admiten el almacén de instancias para el dispositivo raíz.

Las AMI de Windows que se han configurado para una inicialización más rápida con EC2 Fast Launch se aprovisionan previamente mediante el uso de instantáneas a fin de iniciar instancias hasta un 65 % más rápido. Para obtener más información sobre EC2 Fast Launch, consulte Uso del lanzamiento rápido de EC2 para sus instancias de Windows.

> **Note**
>
> Microsoft ya no admite versiones de Windows Server anteriores a Windows Server 2016. Le recomendamos que lance instancias de EC2 nuevas con una versión de Windows Server que tenga soporte. Si aún tiene instancias de EC2 en las que se ejecuta una versión sin soporte de Windows Server, le recomendamos que las actualice a una versión de Windows Server con soporte. Para obtener más información, consulte Actualizar una instancia de Windows Amazon EC2 a una versión más reciente de Windows Server.

Tipos de AMI

Puede elegir la AMI que va a utilizar en función de las características siguientes:

- Región (consulte Regiones y zonas)
- Sistema operativo
- Arquitectura (32 bits o 64 bits)
- Permisos de inicialización
- Almacenamiento para el dispositivo raíz

Permisos de inicialización

El propietario de la AMI determina su disponibilidad especificando permisos de inicialización. Los permisos de inicialización se dividen en las categorías siguientes.

Permiso de inicialización	Descripción
público	El propietario concede permisos de inicialización a todas las cuentas de AWS.
explícito	El propietario concede permisos de inicialización a cuentas de AWS, organizaciones o unidades organizativas (OU) específicas.
implícito	El propietario posee permisos de inicialización implícitos de una AMI.

Amazon y la comunidad de Amazon EC2 ofrecen una amplia selección de AMI públicas. Para obtener más información, consulte AMI compartidas. Los desarrolladores podrían cobrar una tarifa por sus AMI. Para obtener más información, consulte AMI de pago.

Almacenamiento para el dispositivo raíz

Todas las AMI tienen respaldo en Amazon EBS o respaldo en el almacén de instancias.

- AMI basada en Amazon EBS: el dispositivo raíz de una instancia iniciada desde la AMI es un volumen de Amazon Elastic Block Store (Amazon EBS) creado a partir de una instantánea de Amazon EBS. Compatible con AMI de Linux y Windows.
- AMI con almacenamiento de instancias de Amazon: el dispositivo raíz de una instancia iniciada desde la AMI es un volumen de almacén de instancias creado a partir de una plantilla almacenada en Amazon S3. Solo es compatible con las AMI de Linux. Las AMI de Windows no admiten el almacén de instancias para el dispositivo raíz.

Para obtener más información, consulte Volumen raíz de la instancia de Amazon EC2.

En la tabla siguiente se resumen las diferencias importantes a la hora de usar los dos tipos de AMI.

Característica	AMI respaldada por Amazon EBS	AMI con respaldo en el almacenamiento de la instancia de Amazon
Tiempo de arranque de una instancia	Normalmente menos de 1 minuto	Normalmente menos de 5 minutos
Límite de tamaño para un dispositivo raíz	64 TiB**	10 GiB
Volumen de dispositivo raíz	Volumen de EBS	Volumen de almacén de instancia s
Persistencia de datos	De manera predeterminada, el volumen raíz se elimina cuando la instancia termina.* Los datos	Los datos en cualquier volumen de almacenes de instancias se

Característica	AMI respaldada por Amazon EBS	AMI con respaldo en el almacenamiento de la instancia de Amazon
	en cualquier otro volumen de EBS persisten después de la terminación de la instancia de manera predeterminada.	conservan solo durante el ciclo de vida de la instancia.
Modificaciones	El tipo de instancia, el kernel, el disco de la RAM y los datos de usuario se pueden cambiar cuando la instancia está detenida.	Los atributos de instancia son invariables durante el ciclo de vida de una instancia.
Cargos	Se cobra por el uso de la instancia, por el uso del volumen de EBS y por almacenar la AMI como una instantánea de EBS.	Se cobra por el uso de la instancia y por almacenar la AMI en Amazon S3.
Creación y agrupación de AMI	Utiliza un solo comando/llamada	Hay que instalarlo y utilizar herramientas de AMI
Estado detenido	Puede estar en un estado detenido. Incluso cuando la instancia se detiene y no se ejecuta, el volumen raíz persiste en Amazon EBS	No puede estar en el estado detenido; las instancias están ejecutándose o se han terminado

*De forma predeterminada, los volúmenes raíz de EBS tienen el indicador `DeleteOnTermination` establecido en `true`. Para obtener más información acerca de cómo cambiar este indicador para que el volumen se conserve hasta la terminación, consulte Cambiar el volumen raíz a para que persista.

**Solo es compatible con `io2` Block Express de EBS. Para obtener más información, consulte Volúmenes SSD de IOPS aprovisionadas (io2) Block Express en la Guía del usuario de Amazon EBS.

Determinar el tipo de dispositivo raíz de su AMI

Para determinar el tipo de dispositivo raíz de una AMI con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija AMI y, a continuación, seleccione la AMI.
3. En la pestaña Detalles, verifique el valor de Tipo de dispositivo raíz de la siguiente manera:
   - `ebs`: se trata de una AMI respaldada por EBS.
   - `instance store`: se trata de una AMI con almacenamiento de instancias.

Para determinar el tipo de dispositivo raíz de una AMI con la línea de comando

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

- describe-images (AWS CLI)
- Get-EC2Image (AWS Tools for Windows PowerShell)

Estado detenido

Puede detener una instancia que tiene un volumen de EBS para su dispositivo raíz, pero no puede detener una instancia que tiene un volumen de almacén de instancias para su dispositivo raíz.

Al pararse, la instancia deja de ejecutarse (su estado pasa de `running` a `stopping` y a `stopped`). La instancia detenida se mantiene en Amazon EBS, por lo que se puede reiniciar. La acción de parada es diferente a la de terminación; no se puede reiniciar una instancia terminada. Dado que las instancias con volumen de almacén de instancias para el dispositivo raíz no se pueden detener, están en ejecución o terminadas. Para obtener más información acerca del proceso y qué se puede hacer cuando una instancia está detenida, consulte Detención e iniciación de una instancia de Amazon EC2.

Persistencia y almacenamiento de datos predeterminados

Las instancias que utilizan un volumen de almacén de instancias para el dispositivo raíz tienen automáticamente disponible el almacén de instancias (el volumen raíz contiene la partición raíz y puede almacenar datos adicionales). Puede agregar almacenamiento persistente a la instancia al vincular uno o varios volúmenes de EBS. Los datos de un volumen de almacenes de instancias se eliminan cuando la instancia falla o termina. Para obtener más información, consulte Volumen de almacén de instancias y vida de los datos.

Las instancias que utilizan Amazon EBS para el dispositivo raíz tienen automáticamente un volumen de EBS adjunto. El volumen aparece en la lista de volúmenes como cualquier otro. En la mayoría de los tipos de instancias, aquellas que tienen un volumen de EBS para el dispositivo raíz no poseen volúmenes de almacenamiento de instancias de forma predeterminada. Puede agregar volúmenes de almacenes de instancias o volúmenes de EBS adicionales mediante una asignación de dispositivos de bloques. Para obtener más información, consulte Mapeos de dispositivos de bloques.

Tiempos de arranque

Las instancias iniciadas desde una AMI con respaldo Amazon EBS se inician más rápido que las instancias iniciadas desde una AMI con respaldo en el almacén de instancias. Cuando se inicia una instancia desde una AMI con respaldo en el almacén de instancias, hay que recuperar todas las partes de Amazon S3 para que la instancia esté disponible. Con una AMI con respaldo de Amazon EBS, para que la instancia esté disponible, solo hay que recuperar de la instantánea las partes necesarias para arrancar la instancia. Sin embargo, el desempeño de una instancia que utiliza un volumen de EBS para su dispositivo raíz es más lento durante el breve periodo en el que se recuperan las partes restantes de la instantánea y se cargan en el volumen. Cuando la instancia se para y se reinicia, se inicia rápidamente, porque el estado se almacena en un volumen de EBS.

Creación de AMI

Para crear AMI para Linux con respaldo de un almacén de instancias, debe crear una AMI desde la instancia en la propia instancia mediante las herramientas de AMI de Amazon EC2. Tenga en cuenta que las AMI de Windows no admiten el almacén de instancias para el dispositivo raíz.

La creación de AMI es mucho más sencilla para AMI con respaldo en Amazon EBS. La acción de la API `CreateImage` crea la AMI con respaldo en Amazon EBS y la registra. También hay un botón en la AWS Management Console que le permite crear una AMI desde una instancia en ejecución. Para obtener más información, consulte Creación de una AMI basada en Amazon EBS.

Cómo se cobra

Para las AMI con respaldo en el almacén de instancias, se cobra por el almacenamiento de las AMI en Amazon S3 y el uso de instancias. Para las AMI con respaldo en Amazon EBS, se cobra por el uso de instancias, por el almacenamiento y el uso del volumen de EBS y por almacenar la AMI como una instantánea de EBS.

Para las AMI con respaldo en el almacén de instancias Amazon EC2, cada vez que se personaliza una AMI y se crea una nueva, todas las partes se almacenan en Amazon S3 por cada AMI. Por lo tanto, el espacio de almacenamiento de cada AMI personalizada es el tamaño completo de la AMI. Para las AMI basadas en Amazon EBS, cada vez que se personaliza una AMI y se crea una nueva, se almacenan solo los cambios. Por tanto, la huella de almacenamiento de las AMI posteriores que personalice después de la primera es mucho menor, por lo que los cargos de almacenamiento de AMI son menores.

Cuando se detiene una instancia con un volumen de EBS como dispositivo de raíz, no se cobra por el uso de la instancia, sino que se cobra por el almacenamiento del volumen. En cuanto inicie la instancia, cobramos un cargo mínimo de un minuto por uso. Después del primer minuto, solo cobramos por los segundos utilizados. Por ejemplo, si ejecuta una instancia durante 20 segundos y luego la detiene, pasaremos un cargo por un minuto completo. Si ejecuta una instancia durante 3 minutos y 40 segundos, libramos un cargo equivalente exactamente a 3 minutos y 40 segundos de uso. Cobramos por cada segundo, con un mínimo de un minuto, que mantenga la instancia en ejecución, aun cuando permanezca inactiva y no se conecte a ella.

Tipos de virtualización de AMI

Las Imágenes de máquina de Amazon utilizan uno de los dos tipos de virtualización: paravirtual (PV) o máquina virtual de hardware (HVM). Las principales diferencias entre las AMI PV y HVM son el modo de arranque y si admiten extensiones de hardware especiales (CPU, red y almacenamiento) para mejorar su rendimiento. Las AMI de Windows son AMI de HVM.

Para optimizar la inicialización de sus instancias, le recomendamos que utilice los tipos de instancia de la generación actual y las AMI HVM. Para obtener información general sobre los tipos de instancia de la generación actual, consulte Tipos de instancias de Amazon EC2. Si utiliza tipos de instancia de generaciones anteriores y desea actualizar a la versión actual, consulte Vías de actualización y Cambie el tipo de instancia.

En la siguiente tabla se comparan las AMI de HVM y PV.

	HVM	PV
Descripción	Las AMI HVM se presentan con un conjunto de hardware totalmente virtualizado y se cierran ejecutando el Master Boot Record del dispositivo de bloques raíz de la imagen. Este tipo de virtualización ofrece la posibilidad de ejecutar un sistema operativo directamente en una máquina virtual sin ninguna modificación, como si se ejecutara en el propio hardware bare metal. El sistema host de Amazon EC2 emula una parte o todo el hardware subyacente que se presenta al invitado.	Las AMI PV arrancan con un cargador de arranque especial llamado PV-GRUB, que inicia el ciclo de arranque y, a continuación, carga en cadena el kernel especificado en el archivo `menu.lst` de la imagen. Los invitados paravirtuales pueden ejecutarse en hardware host que no tenga compatibilidad explícita para la virtualización. Antes, el rendimiento de los invitados PV era mejor que el de los invitados HVM en muchos casos, pero esto ya no es así debido a las mejoras de la virtualización HVM y a la disponibilidad de controladores PV para AMI HVM. Para obtener más información sobre PV-GRUB y su utilización en Amazon EC2, consulte User provided kernels.
Compatibilidad para extensiones de hardware	Sí. A diferencia de los invitados PV, los invitados HVM pueden beneficiarse de las extensiones de hardware que permiten acceder rápidamente al hardware subyacente del sistema host. Para obtener más información acerca de	No, no pueden aprovechar las extensiones de hardware especiales, como la red mejorada o el procesamiento de GPU.

	HVM	PV
	las extensiones de virtualización de CPU disponibles en Amazon EC2, consulte Tecnología de virtualización Intel en el sitio web de Intel. Además, las AMI HVM son necesarias para beneficiarse de la conexión en red mejorada y del procesamiento de GPU. A fin de transferir las instrucciones a la red especializada y a los dispositivos GPU, el SO necesita obtener acceso a la plataforma de hardware nativa; la virtualización HVM proporciona dicho acceso. Para obtener más información, consulte Redes mejoradas en Amazon EC2.	
Tipos de instancias admitidos	Todos los tipos de instancia de la generación actual admiten AMI HVM.	Los siguientes tipos de instancia de generaciones anteriores admiten AMI PV: C1, C3, M1, M3, M2 y T1. Los tipos de instancia de la generación actual no admiten AMI PV.

	HVM	PV
Regiones admitidas	Todas las regiones admiten instancias de HVM.	Asia Pacífico (Tokio), Asia Pacífico (Singapur), Asia Pacífico (Sídney), Europa (Fráncfort), Europa (Irlanda), América del Sur (São Paulo), US East (N. Virginia), EE.UU. Oeste (Norte de California) y EE.UU. Oeste (Oregón)
Cómo encontrar	Verifique que el tipo de virtualización de la AMI esté configurado en `hvm`, mediante la consola o el comando describe-images. Para obtener más información, consulte Buscar una AMI.	Verifique que el tipo de virtualización de la AMI esté configurado en `paravirtual`, mediante la consola o el comando describe-images. Para obtener más información, consulte Buscar una AMI.

PV frente a HVM

Tradicionalmente, los invitados paravirtuales tenían un mejor desempeño en las operaciones de almacenamiento y redes que los invitados HVM porque podían hacer uso de controladores especiales para E/S que evitaban el costo adicional de tener que emular hardware de red y de disco, mientras que los invitados HVM tenían que traducir estas instrucciones en un hardware emulado. Actualmente, estos controladores PV están disponibles para invitados HVM, de forma que, si un sistema operativo no se puede transferir para ejecutarse en un entorno paravirtualizado, aún puede usar estos controladores para optimizar la E/S de las redes y el almacenamiento. Además, con los controladores PV para HVM, los invitados HVM obtienen el mismo rendimiento, o incluso mejor, que con los invitados paravirtuales.

Modos de arranque de Amazon EC2

Cuando se inicia una computadora, el primer software que ejecuta se encarga de inicializar la plataforma y proporcionar una interfaz para que el sistema operativo realice operaciones específicas de la plataforma.

En Amazon EC2, se admiten dos variantes del software de modo de arranque: Legacy BIOS y Unified Extensible Firmware Interface (UEFI).

Posibles parámetros de modo de arranque en una AMI

Una AMI puede tener uno de los siguientes valores de parámetro de modo de arranque: `uefi`, `legacy-bios` o `uefi-preferred`. El parámetro de modo de arranque de la AMI es opcional. En las AMI que no tienen ningún parámetro de modo de arranque, las instancias iniciadas desde estas AMI utilizan el valor de modo de arranque predeterminado del tipo de instancia.

Finalidad del parámetro de modo de arranque de la AMI

El parámetro de modo de arranque de la AMI indica a Amazon EC2 qué modo de arranque se debe utilizar cuando se inicia una instancia. Cuando el parámetro de modo de arranque se establece en `uefi`, EC2 intenta iniciar la instancia en UEFI. Si el sistema operativo no se encuentra configurado para admitir UEFI, la instancia no se iniciará correctamente.

Parámetro de modo de arranque preferido UEFI

Puede crear AMI que admitan UEFI y BIOS heredados mediante el parámetro del modo de arranque `uefi-preferred`. Cuando el parámetro de modo de arranque se establece en `uefi-preferred` y el tipo de instancia admite UEFI, la instancia se inicia en UEFI. Si el tipo de instancia no admite UEFI, la instancia se inicia en un BIOS heredado.

> **Warning**
>
> Algunas características, como UEFI Secure Boot, solo están disponibles en instancias que arrancan en UEFI. Al utilizar el parámetro del modo de arranque de AMI `uefi-preferred` con un tipo de instancia que no admita UEFI, la instancia se iniciará como BIOS antigua y la característica dependiente de UEFI se deshabilitará. Si confía en la disponibilidad de una característica dependiente de UEFI, defina el parámetro del modo de arranque de AMI en `uefi`.

Modos de arranque predeterminados para los tipos de instancias

- Tipos de instancia de Graviton: UEFI
- Tipos de instancias de Intel y AMD: Legacy BIOS

Ejecución de tipos de instancias Intel y AMD en UEFI

Most Intel and AMD instance types puede ejecutarse tanto en UEFI como en Legacy BIOS. Para utilizar UEFI, debe seleccionar una AMI con el parámetro de modo de arranque establecido en `uefi` o `uefi-preferred` y el sistema operativo de la AMI debe estar configurado para admitir UEFI.

Temas sobre el modo de arranque

- Iniciar una instancia
- Determinar el parámetro de modo de arranque de una AMI
- Determinar los modos de arranque que admite un tipo de instancia
- Determinar el modo de arranque de una instancia
- Determinar el modo de arranque del sistema operativo
- Establezca el modo de arranque de una AMI
- Variables UEFI
- Arranque seguro UEFI

Iniciar una instancia

Puede iniciar una instancia en modo de arranque UEFI o Legacy BIOS.

Temas

- Limitaciones
- Consideraciones
- Requisitos para iniciar una instancia en UEFI

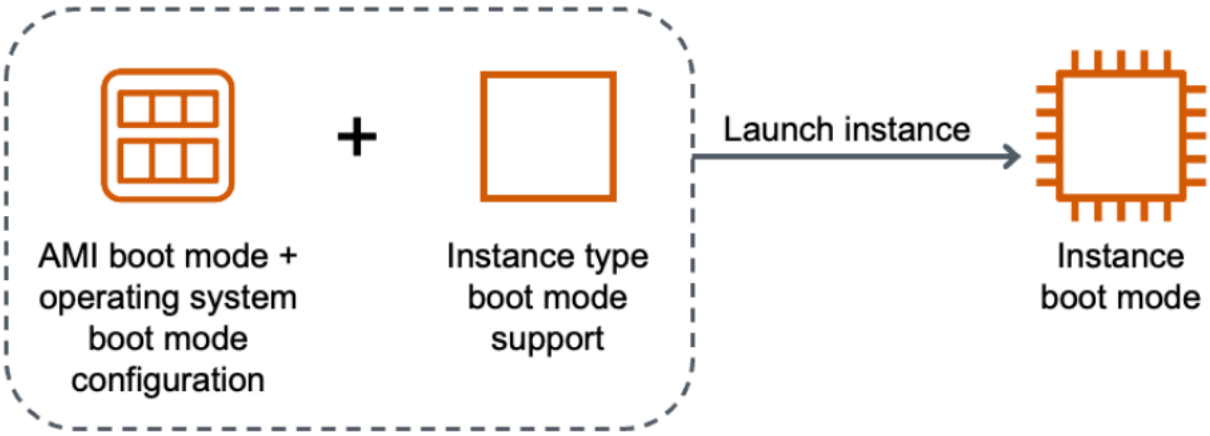
Limitaciones

El arranque UEFI no es compatible en zonas locales, Wavelength o con AWS Outposts.

Consideraciones

A la hora de iniciar una instancia, tenga en cuenta lo siguiente:

- El modo de arranque de la instancia viene determinado por la configuración de la AMI, el sistema operativo que contiene y el tipo de instancia, como se muestra en la siguiente imagen:



En la siguiente tabla se muestra que el modo de arranque de una instancia (indicado en la columna Modo de arranque de la instancia resultante) se determina mediante una combinación del parámetro de modo de arranque de la AMI (columna 1), la configuración del modo de arranque del sistema operativo de la AMI (columna 2) y la compatibilidad con el modo de arranque del tipo de instancia (columna 3).

Parámetro de modo de arranque AMI	Configuración de modo de arranque del sistema operativo	Compatibilidad del modo de arranque del tipo de instancia	Modo de arranque de la instancia resultante
UEFI	UEFI	UEFI	UEFI
BIOS antigua	BIOS antigua	BIOS antigua	BIOS antigua
UEFI preferida	UEFI	UEFI	UEFI
UEFI preferida	UEFI	UEFI y BIOS heredado	UEFI
UEFI preferida	BIOS antigua	BIOS antigua	BIOS antigua
UEFI preferida	BIOS antigua	UEFI y BIOS antigua	BIOS antigua
No se especificó ningún modo de arranque: ARM	UEFI	UEFI	UEFI

Parámetro de modo de arranque AMI	Configuración de modo de arranque del sistema operativo	Compatibilidad del modo de arranque del tipo de instancia	Modo de arranque de la instancia resultante
No se especificó ningún modo de arranque: x86	BIOS antigua	UEFI y BIOS antigua	BIOS antigua

- Modos de arranque predeterminados:
  - Tipos de instancia de Graviton: UEFI
  - Tipos de instancias de Intel y AMD: Legacy BIOS
- Tipos de instancias Intel y AMD compatibles con UEFI, además de Legacy BIOS:
  - Todas las instancias integradas en AWS Nitro System, excepto: instancias bare metal, DL1, G4ad, P4, u-3tb1, u-6tb1, u-9tb1, u-12tb1, u-18tb1, u-24tb1 y VT1.

Para ver los tipos de instancias disponibles que son compatibles con UEFI en una región específica

Los tipos de instancia disponibles varían según Región de AWS. Para ver los tipos de instancias disponibles que son compatibles con UEFI en una región, utilice el comando describe-instance-types con el parámetro `--region`. Si omite el parámetro `--region`, se utilizará su región predeterminada en la solicitud. Incluya el parámetro `--filters` a fin de limitar los resultados a los tipos de instancia que admiten UEFI y el parámetro `--query` para limitar la salida al valor de `InstanceType`.

Utilice el comando correspondiente a su sistema operativo.

Linux

AWS CLI

```
$ aws ec2 describe-instance-types --filters Name=supported-boot-mode,Values=uefi --
query "InstanceTypes[*].[InstanceType]" --output text | sort

a1.2xlarge
a1.4xlarge
a1.large
a1.medium
a1.metal
```

```
a1.xlarge
c5.12xlarge
...
```

PowerShell

```
PS C:\> Get-EC2InstanceType | `
 Where-Object {$_.SupportedBootModes -Contains "uefi"} | `
 Sort-Object InstanceType | `
 Format-Table InstanceType -GroupBy CurrentGeneration

CurrentGeneration: False

InstanceType
------------
a1.2xlarge
a1.4xlarge
a1.large
a1.medium
a1.metal
a1.xlarge

CurrentGeneration: True

InstanceType
------------
c5.12xlarge
c5.18xlarge
c5.24xlarge
c5.2xlarge
c5.4xlarge
c5.9xlarge
...
```

Windows

AWS CLI

```
$ aws ec2 describe-instance-types --filters Name=supported-boot-mode,Values=uefi
 Name=processor-info.supported-architecture,Values=x86_64 --query "InstanceTypes[*].
[InstanceType]" --output text | sort
```

```
c5.12xlarge
c5.18xlarge
c5.24xlarge
c5.2xlarge
c5.4xlarge
c5.9xlarge
c5.large
...
```

PowerShell

```
PS C:\> Get-EC2InstanceType | `
 Where-Object {
     $_.SupportedBootModes -Contains "uefi" -and `
     $_.ProcessorInfo.SupportedArchitectures -eq "x86_64"
     } | `
 Sort-Object InstanceType | `
 Format-Table InstanceType -GroupBy CurrentGeneration

CurrentGeneration: True

InstanceType
------------
c5.12xlarge
c5.18xlarge
c5.24xlarge
c5.2xlarge
c5.4xlarge
...
```

Para ver los tipos de instancias disponibles que son compatibles con UEFI Secure Boot y con variables no volátiles persistentes en una región específica

Actualmente, las instancias bare metal no admiten UEFI Secure Boot ni variables no volátiles. Utilice el comando describe-instance-types como se explica en el ejemplo anterior, pero filtre las instancias bare metal por medio del filtro `Name=bare-metal,Values=false`. Para obtener más información sobre el arranque seguro UEFI, consulte Arranque seguro UEFI.

Utilice el comando correspondiente a su sistema operativo.

Linux

AWS CLI

```
$ aws ec2 describe-instance-types --filters Name=supported-boot-mode,Values=uefi
 Name=bare-metal,Values=false --query "InstanceTypes[*].[InstanceType]" --output
 text | sort

a1.2xlarge
a1.4xlarge
a1.large
a1.medium
...
```

PowerShell

```
PS C:\> Get-EC2InstanceType | `
    Where-Object { `
        $_.SupportedBootModes -Contains "uefi" -and `
        $_.BareMetal -eq $False
        } | `
    Sort-Object InstanceType  | `
    Format-Table InstanceType, SupportedBootModes, BareMetal,
 @{Name="SupportedArchitectures";
 Expression={$_.ProcessorInfo.SupportedArchitectures}}

InstanceType     SupportedBootModes  BareMetal SupportedArchitectures
------------     ------------------  --------- ----------------------
a1.2xlarge       {uefi}                  False arm64
a1.4xlarge       {uefi}                  False arm64
a1.large         {uefi}                  False arm64
a1.medium        {uefi}                  False arm64
a1.xlarge        {uefi}                  False arm64
c5.12xlarge      {legacy-bios, uefi}     False x86_64
c5.18xlarge      {legacy-bios, uefi}     False x86_64
```

Windows

AWS CLI

```
$ aws ec2 describe-instance-types --filters Name=supported-boot-
mode,Values=uefi Name=bare-metal,Values=false Name=processor-info.supported-
```

```
architecture,Values=x86_64 --query "InstanceTypes[*].[InstanceType]" --output text |
 sort

c5.12xlarge
c5.18xlarge
c5.24xlarge
c5.2xlarge
...
```

PowerShell

```
PS C:\> Get-EC2InstanceType | `
    Where-Object { `
        $_.SupportedBootModes -Contains "uefi" -and `
        $_.BareMetal -eq $False -and `
        $_.ProcessorInfo.SupportedArchitectures -eq "x86_64"
        } | `
    Sort-Object InstanceType  | `
    Format-Table InstanceType, SupportedBootModes, BareMetal,
 @{Name="SupportedArchitectures";
 Expression={$_.ProcessorInfo.SupportedArchitectures}}

InstanceType    SupportedBootModes  BareMetal SupportedArchitectures
------------    ------------------  --------- ----------------------
c5.12xlarge     {legacy-bios, uefi}     False x86_64
c5.18xlarge     {legacy-bios, uefi}     False x86_64
c5.24xlarge     {legacy-bios, uefi}     False x86_64
c5.2xlarge      {legacy-bios, uefi}     False x86_64
c5.4xlarge      {legacy-bios, uefi}     False x86_64
c5.9xlarge      {legacy-bios, uefi}     False x86_64
```

Requisitos para iniciar una instancia en UEFI

Para iniciar una instancia en modo de arranque UEFI, debe seleccionar un tipo de instancia que admita UEFI y configurar la AMI y el sistema operativo para UEFI de la siguiente manera:

Tipo de instancia

Cuando lance una instancia, debe seleccionar un tipo de instancia que admita UEFI. Para obtener más información, consulte Determinar los modos de arranque que admite un tipo de instancia.

AMI

Cuando lance una instancia, debe seleccionar una AMI que esté configurada para UEFI. La AMI debe configurarse de la siguiente manera:

- Sistema operativo: el sistema operativo contenido en la AMI debe configurarse de forma que utilice UEFI. De lo contrario, se producirá un error en la inicialización de la instancia. Para obtener más información, consulte Determinar el modo de arranque del sistema operativo.
- Parámetro de modo de arranque de la AMI: el parámetro de modo de arranque de la AMI debe establecerse en `uefi` o `uefi-preferred`. Para obtener más información, consulte Determinar el parámetro de modo de arranque de una AMI.

Linux: AWS solo proporciona AMI de Linux configuradas para admitir UEFI para tipos de instancias basadas en Graviton. Para utilizar Linux en otros tipos de instancia UEFI, debe configurar la AMI, importar la AMI a través de VM Import/Export o importar la AMI a través de CloudEndure.

Windows: las siguientes AMI de Windows admiten UEFI:

- TPM-Windows_Server-2022-English-Full-Base
- TPM-Windows_Server-2022-English-Core-Base
- TPM-Windows_Server-2019-English-Full-Base
- TPM-Windows_Server-2019-English-Core-Base
- TPM-Windows_Server-2016-English-Full-Base
- TPM-Windows_Server-2016-English-Core-Base

Determinar el parámetro de modo de arranque de una AMI

El parámetro de modo de arranque de la AMI es opcional. Una AMI puede tener uno de los siguientes valores de parámetro de modo de arranque: `uefi`, `legacy-bios` o `uefi-preferred`.

Algunas AMI no tienen un parámetro de modo de arranque. Cuando una AMI no tiene ningún parámetro de modo de arranque, las instancias iniciadas desde la AMI utilizan el valor predeterminado del tipo de instancia, que es `uefi` en Graviton y `legacy-bios` en los tipos de instancias de Intel y AMD.

Console

Para determinar el parámetro de modo de arranque de una AMI (consola)

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija AMI y, a continuación, seleccione la AMI.
3. Inspeccione el campo Modo de arranque.
   - El valor uefi indica que la AMI es compatible con UEFI.
   - El valor uefi-preferred indica que la AMI es compatible con UEFI y el BIOS heredado.
   - Si no hay ningún valor, las instancias iniciadas desde la AMI utilizan el valor predeterminado del tipo de instancia.

Para determinar el parámetro de modo de arranque de una AMI cuando se inicia una instancia (consola)

Cuando lance una instancia mediante el asistente de inicialización de instancias, en el paso para seleccionar una AMI, examine el campo Modo de arranque. Para obtener más información, consulte Imágenes de aplicaciones y sistema operativo (Imagen de máquina de Amazon).

AWS CLI

Para determinar el parámetro de modo de arranque de una AMI (AWS CLI)

Utilice la operación describe-images para determinar el modo de arranque de una AMI.

```
aws ec2 describe-images --region us-east-1 --image-id ami-0abcdef1234567890

{
    "Images": [
        {
         ...
            ],
            "EnaSupport": true,
            "Hypervisor": "xen",
            "ImageOwnerAlias": "amazon",
            "Name": "UEFI_Boot_Mode_Enabled-Windows_Server-2016-English-Full-
Base-2020.09.30",
            "RootDeviceName": "/dev/sda1",
            "RootDeviceType": "ebs",
            "SriovNetSupport": "simple",
```

```
            "VirtualizationType": "hvm",
            "BootMode":
 "uefi"
        }
    ]
}
```

En la salida, el campo `BootMode` indica el modo de arranque de la AMI. Un valor de `uefi` indica que la AMI es compatible con UEFI. Un valor de `uefi-preferred` indica que la AMI es compatible con UEFI y la BIOS antigua. Si no hay ningún valor, las instancias iniciadas desde la AMI utilizan el valor predeterminado del tipo de instancia.

PowerShell

Para determinar el parámetro de modo de arranque de una AMI (herramientas para PowerShell)

Utilice el Cmdlet Get-EC2Image para determinar el modo de arranque de una AMI.

```
PS C:\> Get-EC2Image -Region us-east-1 -ImageId ami-0abcdef1234567890 | Format-List
 Name, BootMode, TpmSupport

Name       : TPM-Windows_Server-2016-English-Full-Base-2023.05.10
BootMode   : uefi
TpmSupport : v2.0
```

En la salida, el campo `BootMode` indica el modo de arranque de la AMI. Un valor de `uefi` indica que la AMI es compatible con UEFI. Un valor de `uefi-preferred` indica que la AMI es compatible con UEFI y la BIOS antigua. Si no hay ningún valor, las instancias iniciadas desde la AMI utilizan el valor predeterminado del tipo de instancia.

Determinar los modos de arranque que admite un tipo de instancia

Puede usar el AWS CLI olas herramientas para PowerShell para determinar los modos de arranque que admite un tipo de instancia.

Para determinar los modos de arranque que admite un tipo de instancia

Puede usar los siguientes métodos para determinar los modos de arranque que admite un tipo de instancia.

AWS CLI

Puede usar el comando describe-instance-types para determinar los modos de arranque que admite un tipo de instancia. Al incluir el parámetro `--query`, puede filtrar la salida. En este ejemplo, la salida se filtra para devolver solo los modos de arranque admitidos.

En el siguiente ejemplo se muestra que `m5.2xlarge` es compatible con los modos de arranque UEFI y BIOS heredado.

```
aws ec2 describe-instance-types --region us-east-1 --instance-types m5.2xlarge --
query "InstanceTypes[*].SupportedBootModes"
```

Resultado previsto:

```
[
    [
        "legacy-bios",
        "uefi"
    ]
]
```

En el siguiente ejemplo se muestra que solo `t2.xlarge` es compatible con el BIOS heredado.

```
aws ec2 describe-instance-types --region us-east-1 --instance-types t2.xlarge --
query "InstanceTypes[*].SupportedBootModes"
```

Resultado previsto:

```
[
    [
        "legacy-bios"
    ]
]
```

PowerShell

Puede usar el Cmdlet Get-EC2InstanceType (herramientas para PowerShell) para determinar los modos de arranque que admite un tipo de instancia.

En el siguiente ejemplo se muestra que `m5.2xlarge` es compatible con los modos de arranque UEFI y BIOS heredado.

```
Get-EC2InstanceType -Region us-east-1 -InstanceType m5.2xlarge | Format-List
 InstanceType, SupportedBootModes
```

Resultado previsto:

```
InstanceType       : m5.2xlarge
SupportedBootModes : {legacy-bios, uefi}
```

En el siguiente ejemplo se muestra que solo `t2.xlarge` es compatible con el BIOS heredado.

```
Get-EC2InstanceType -Region us-east-1 -InstanceType t2.xlarge | Format-List
 InstanceType, SupportedBootModes
```

Resultado previsto:

```
InstanceType       : t2.xlarge
SupportedBootModes : {legacy-bios}
```

Determinar el modo de arranque de una instancia

El modo de arranque de una instancia se muestra en el campo Modo de arranque de la consola de Amazon EC2 y junto al parámetro `currentInstanceBootMode` de AWS CLI.

Cuando se inicia una instancia, el valor de su parámetro de modo de arranque se determina mediante el valor del parámetro de modo de arranque de la AMI utilizada para iniciarla, de la siguiente manera:

- Una AMI con un parámetro de modo de arranque de `uefi` crea una instancia con un parámetro `currentInstanceBootMode` de `uefi`.
- Una AMI con un parámetro de modo de arranque de `legacy-bios` crea una instancia con un parámetro `currentInstanceBootMode` de `legacy-bios`.
- Una AMI con un parámetro de modo de arranque de `uefi-preferred` crea una instancia con un parámetro `currentInstanceBootMode` de `uefi` si el tipo de instancia admite UEFI; de lo contrario, crea una instancia con un parámetro `currentInstanceBootMode` de `legacy-bios`.
- Una AMI sin valor de parámetro de modo de arranque crea una instancia con un valor de parámetro `currentInstanceBootMode` que depende de si la arquitectura de la AMI es ARM o

x86 y del modo de arranque admitido del tipo de instancia. El modo de arranque predeterminado es `uefi` en los tipos de instancia de Graviton y `legacy-bios` en los tipos de instancia de Intel y AMD.

Console

Para determinar el modo de arranque de una instancia (consola)

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instances (instancia[s]) y seleccione la instancia.
3. En la pestaña Detalles, examine el campo Modo de arranque.

AWS CLI

Para determinar el modo de arranque de una instancia (AWS CLI)

Utilice el comando describe-instances para determinar el modo de arranque de una instancia. También puede determinar el modo de arranque de la AMI que se utilizó para crear la instancia.

```
aws ec2 describe-instances --region us-east-1 --instance-ids i-1234567890abcdef0

{
    "Reservations": [
        {
            "Groups": [],
            "Instances": [
                {
                    "AmiLaunchIndex": 0,
                    "ImageId": "ami-0e2063e7f6dc3bee8",
                    "InstanceId": "i-1234567890abcdef0",
                    "InstanceType": "m5.2xlarge",
                    ...
                    },
                   "BootMode": "uefi",
                   "CurrentInstanceBootMode": "uefi"
                }
            ],
            "OwnerId": "1234567890",
            "ReservationId": "r-1234567890abcdef0"
        }
    ]
```

```
}
```

PowerShell

Para determinar el modo de arranque de una instancia (herramientas para PowerShell)

Utilice el Cmdlet Get-EC2Image para determinar el modo de arranque de una instancia. También puede determinar el modo de arranque de la AMI que se utilizó para crear la instancia.

Get-EC2Image (AWS Tools for Windows PowerShell)

```
(Get-EC2Instance -InstanceId i-1234567890abcdef0).Instances | Format-List BootMode,
 CurrentInstanceBootMode, InstanceType, ImageId

BootMode                : uefi
CurrentInstanceBootMode : uefi
InstanceType            : c5a.large
ImageId                 : ami-0265446f88eb4021b
```

En el resultado, los siguientes parámetros describen el modo de arranque:

- `BootMode`: el modo de arranque de la AMI que se utilizó para crear la instancia.
- `CurrentInstanceBootMode`: el modo de arranque que se utiliza para arrancar la instancia en el momento de la inicialización o el inicio.

Determinar el modo de arranque del sistema operativo

El modo de arranque de la AMI indica a Amazon EC2 qué modo de arranque se utiliza para iniciar una instancia. Para ver si el sistema operativo de la instancia está configurado para UEFI, debe conectarse a la instancia mediante SSH (instancias de Linux) or RDP (instancias de Windows).

Consulte las instrucciones del sistema operativo de su instancia.

Linux

Para determinar el modo de arranque del sistema operativo de la instancia

1. Conéctese a su instancia de Linux mediante SSH.
2. Para ver el modo de arranque del sistema operativo, pruebe uno de los siguientes procedimientos:

- Ejecute el siguiente comando.

```
[ec2-user ~]$ sudo /usr/sbin/efibootmgr
```

Resultado esperado de una instancia iniciada con el modo de arranque UEFI

```
BootCurrent: 0001
Timeout: 0 seconds
BootOrder: 0000,0001
Boot0000* UiApp
Boot0001* UEFI Amazon Elastic Block Store vol-xyz
```

- Ejecute el siguiente comando para verificar la existencia del directorio `/sys/firmware/efi`. Este directorio solo existe si la instancia se inicia con UEFI. Si el directorio no existe, el comando devuelve `Legacy BIOS Boot Detected`.

```
[ec2-user ~]$ [ -d /sys/firmware/efi ] && echo "UEFI Boot Detected" || echo
 "Legacy BIOS Boot Detected"
```

Resultado esperado de una instancia iniciada con el modo de arranque UEFI

```
UEFI Boot Detected
```

Resultado esperado de una instancia iniciada con el modo de arranque Legacy BIOS

```
Legacy BIOS Boot Detected
```

- Ejecute el siguiente comando para verificar que EFI aparece en la salida `dmesg`.

```
[ec2-user ~]$ dmesg | grep -i "EFI"
```

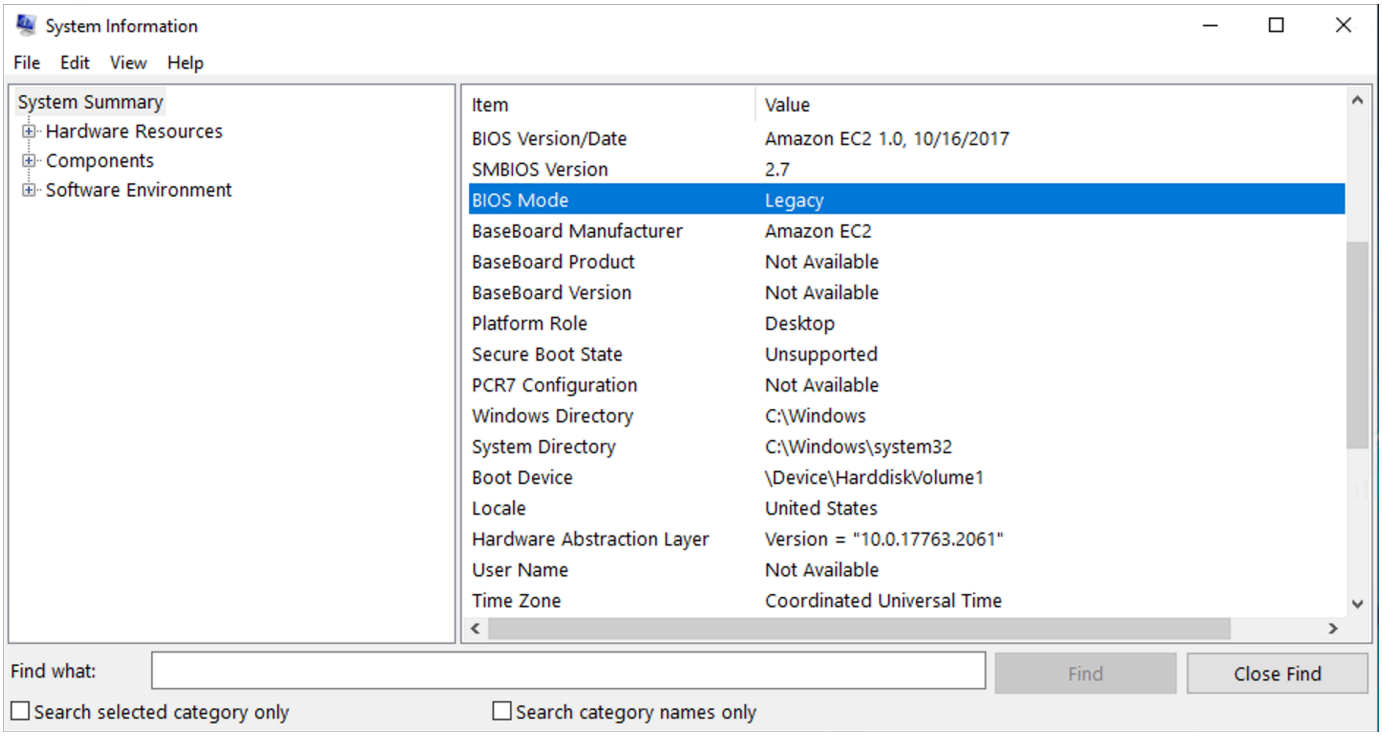
Resultado esperado de una instancia lanzada con el modo de arranque UEFI

```
[    0.000000] efi: Getting EFI parameters from FDT:
[    0.000000] efi: EFI v2.70 by EDK II
```

Windows

Para determinar el modo de arranque del sistema operativo de la instancia

1. Conéctese a la instancia de Windows mediante RDP.
2. Vaya a Información del sistema y consulte la fila Modo BIOS.



Establezca el modo de arranque de una AMI

Cuando crea una AMI mediante el comando register-image, puede establecer el modo de arranque de la AMI en `uefi`, `legacy-bios` o `uefi-preferred`.

Cuando el modo de arranque de la AMI está establecido en `uefi-preferred`, la instancia se inicia de la siguiente manera:

- En el caso de los tipos de instancia que admiten UEFI y BIOS heredado (por ejemplo, `m5.large`), la instancia se inicia mediante UEFI.
- En el caso de los tipos de instancia que únicamente admiten el BIOS heredado (por ejemplo, `m4.large`), la instancia se inicia mediante el BIOS heredado.

> **Note**
>
> Si configura el modo de arranque de la AMI en `uefi-preferred`, el sistema operativo tiene que admitir la posibilidad de arrancar en UEFI y BIOS heredado.
> Actualmente, no puede usar el comando register-image para crear una AMI que sea compatible con NitroTPM y UEFI preferido.

> **Warning**
>
> Algunas características, como UEFI Secure Boot, solo están disponibles en instancias que arrancan en UEFI. Al utilizar el parámetro del modo de arranque de AMI `uefi-preferred` con un tipo de instancia que no admita UEFI, la instancia se iniciará como BIOS antigua y la característica dependiente de UEFI se deshabilitará. Si depende de la disponibilidad de una característica dependiente de UEFI, defina el parámetro del modo de arranque de AMI en `uefi`.

Para convertir una instancia existente basada en Legacy BIOS en UEFI o una instancia existente basada en UEFI en Legacy BIOS debe realizar una serie de pasos. Primero, modifique el volumen y el sistema operativo de la instancia para admitir el modo de arranque seleccionado. Luego, cree una instantánea del volumen. Por último, utilice register-image para crear la AMI con la instantánea.

No se puede establecer el modo de arranque de una AMI con el comando create-image. Con create-image, la AMI hereda el modo de arranque de la instancia de EC2 utilizada para crear la AMI. Por ejemplo, si crea una AMI a partir de una instancia de EC2 que se ejecuta en Legacy BIOS, el modo de arranque de la AMI que se configurará será `legacy-bios`. Si crea una AMI a partir de una instancia de EC2 que se lanzó mediante una AMI con un modo de arranque establecido en `uefi-preferred`, la AMI que se cree también tendrá su modo de arranque establecido en `uefi-preferred`.

> **Warning**
>
> Establecer el parámetro de modo de arranque de la AMI no configura automáticamente el sistema operativo para el modo de arranque especificado. Antes de continuar con estos pasos, primero debe realizar las modificaciones adecuadas en el volumen y el sistema operativo de la instancia para admitir el arranque mediante el modo de arranque seleccionado. De lo contrario, no se podrá utilizar la AMI obtenida. Por ejemplo,

si está convirtiendo una instancia basada en Legacy BIOS a UEFI, puede utilizar la herramienta MBR2GPT de Microsoft para convertir el disco del sistema de MBR a GPT. Las modificaciones obligatorias son específicas del sistema operativo. Para obtener más información, consulte el manual del sistema operativo.

Para establecer el modo de arranque de una AMI (AWS CLI)

1. Realice las modificaciones adecuadas en el volumen y el sistema operativo de la instancia para admitir el arranque a través del modo de arranque seleccionado. Las modificaciones obligatorias son específicas del sistema operativo. Para obtener más información, consulte el manual del sistema operativo.

   > **Note**
   >
   > Si no realiza este paso, no se podrá utilizar la AMI.

2. Para buscar el ID de volumen de la instancia, utilice el comando describe-instances. En el siguiente paso, creará una instantánea de este volumen.

   ```
   aws ec2 describe-instances --region us-east-1 --instance-ids i-1234567890abcdef0
   ```

   Resultado previsto

   ```
   ...
               "BlockDeviceMappings": [
                           {
                               "DeviceName": "/dev/sda1",
                               "Ebs": {
                                   "AttachTime": "",
                                   "DeleteOnTermination": true,
                                   "Status": "attached",
                                   "VolumeId": "vol-1234567890abcdef0"
                               }
                           }
                           ...
   ```

3. Para crear una instantánea del volumen, utilice el comando create-snapshot. Utilice el ID del volumen del paso anterior.

```
aws ec2 create-snapshot --region us-east-1 --volume-id vol-1234567890abcdef0 --
description "add text"
```

Salida prevista

```
{
 "Description": "add text",
 "Encrypted": false,
 "OwnerId": "123",
 "Progress": "",
 "SnapshotId": "snap-01234567890abcdef",
 "StartTime": "",
 "State": "pending",
 "VolumeId": "vol-1234567890abcdef0",
 "VolumeSize": 30,
 "Tags": []
}
```

4. Anote el ID de instantánea del resultado del paso anterior.
5. Espere hasta que la creación de la instantánea se encuentre en estado `completed` antes de ir al siguiente paso. Para consultar el estado de la instantánea, utilice el comando describe-snapshots.

```
aws ec2 describe-snapshots --region us-east-1 --snapshot-ids snap-01234567890abcdef
```

Ejemplo de resultado

```
{
    "Snapshots": [
        {
            "Description": "This is my snapshot",
            "Encrypted": false,
            "VolumeId": "vol-049df61146c4d7901",
            "State": "completed",
            "VolumeSize": 8,
            "StartTime": "2019-02-28T21:28:32.000Z",
            "Progress": "100%",
            "OwnerId": "012345678910",
            "SnapshotId": "snap-01234567890abcdef",
...
```

6. Para crear una AMI, utilice el comando register-image. Utilice el ID de la instantánea que anotó en el paso anterior.

   - Para configurar el modo de arranque en UEFI, agregue el parámetro `--boot-mode` al comando y especifique `uefi` como valor.

```
aws ec2 register-image \
   --region us-east-1 \
   --description "add description" \
   --name "add name" \
   --block-device-mappings "DeviceName=/dev/
sda1,Ebs={SnapshotId=snap-01234567890abcdef,DeleteOnTermination=true}" \
   --architecture x86_64 \
   --root-device-name /dev/sda1 \
   --virtualization-type hvm \
   --ena-support \
   --boot-mode uefi
```

   - Para configurar el modo de arranque en `uefi-preferred`, agregue el parámetro `--boot-mode` al comando y especifique `uefi-preferred` como valor.

```
aws ec2 register-image \
   --region us-east-1 \
   --description "add description" \
   --name "add name" \
   --block-device-mappings "DeviceName=/dev/
sda1,Ebs={SnapshotId=snap-01234567890abcdef,DeleteOnTermination=true}" \
   --architecture x86_64 \
   --root-device-name /dev/sda1 \
   --virtualization-type hvm \
   --ena-support \
   --boot-mode uefi-preferred
```

   Resultado previsto

```
{
"ImageId": "ami-new_ami_123"
}
```

7. Para verificar que la AMI recién creada cuenta el modo de arranque especificado en el paso anterior, utilice el comando describe-images.

```
aws ec2 describe-images --region us-east-1 --image-id ami-new_ami_123
```

Resultado previsto

```
{
  "Images": [
   {
   "Architecture": "x86_64",
   "CreationDate": "2021-01-06T14:31:04.000Z",
   "ImageId": "ami-new_ami_123",
   "ImageLocation": "",
   ...
   "BootMode": "uefi"
   }
   ]
}
```

8. Lance una instancia nueva utilizando la AMI recién creada.

   Si el modo de arranque de la AMI es `uefi` o `legacy-bios`, las instancias creadas a partir de esta AMI tendrán el mismo modo de arranque que la AMI. Si el modo de arranque de la AMI es `uefi-preferred`, la instancia se iniciará mediante UEFI si el tipo de instancia admite UEFI; de lo contrario, la instancia se iniciará con un BIOS heredado. Para obtener más información, consulte Consideraciones.

9. Para verificar que la instancia nueva tiene el modo de arranque esperado, utilice el comando describe-instances.

Variables UEFI

Cuando inicia una instancia en la que el modo de arranque se establece en UEFI, se crea un almacén de clave-valor para variables. La UEFI y el sistema operativo de instancias pueden utilizar el almacén para almacenar variables UEFI.

El cargador de arranque y el sistema operativo utilizan las variables UEFI para configurar el inicio temprano del sistema. Permiten que el sistema operativo administre ciertas configuraciones del proceso de arranque, como la orden de arranque o la administración de claves para el Arranque seguro UEFI.

> **Warning**
>
> Cualquier persona que pueda conectarse a la instancia (y, posiblemente, cualquier software que se ejecute en la instancia) o cualquier persona con permisos para usar la API GetInstanceUefiData en la instancia puede leer las variables. Nunca debe almacenar información confidencial, como contraseñas o información de identificación personal, en el almacén de variables de la UEFI.

Persistencia de las variables UEFI

- En el caso de las instancias que se iniciaron el 10 de mayo de 2022 o en una fecha anterior, las variables UEFI se borran cuando se reinician o detienen.
- En el caso de las instancias que se iniciaron el 11 de mayo de 2022 o en una fecha posterior, las variables UEFI marcadas como no volátiles persisten cuando se reinician, o cuando se inician o detienen.
- Las instancias bare metal no conservan las variables no volátiles de la UEFI en las operaciones de detención o inicio de las instancias.

Arranque seguro UEFI

El modo UEFI Secure Boot se basa en el proceso de arranque seguro consolidado de Amazon EC2 y proporciona protección adicional en profundidad que ayuda a los clientes a proteger el software frente a amenazas que persisten durante los reinicios. Garantiza que la instancia solo arranque el software firmado con claves criptográficas. Las claves se almacenan en la base de datos de claves del almacenamiento variable no volátil de la UEFI. UEFI Secure Boot evita la modificación no autorizada del flujo de arranque de las instancias.

Temas

- Cómo funciona UEFI Secure Boot
- Lance una instancia con soporte de UEFI Secure Boot
- Comprobar si una instancia está habilitada para UEFI Secure Boot
- Crear una AMI de Linux para admitir UEFI Secure Boot
- Cómo se crea el blob binario de AWS

Cómo funciona UEFI Secure Boot

UEFI Secure Boot es una característica especificada en la UEFI, que permite verificar el estado de la cadena de arranque. Está diseñado para garantizar que solo se ejecuten binarios UEFI verificados de manera criptográfica después de la autoinicialización del firmware. Estos binarios incluyen los controladores UEFI y el gestor de arranque principal, así como componentes cargados en cadena.

UEFI Secure Boot especifica cuatro bases de datos clave, que se utilizan en una cadena de confianza. Las bases de datos se almacenan en el almacén de variables UEFI.

La cadena de confianza es la siguiente:

Base de datos de la clave de la plataforma (PK)

La base de datos de PK es la raíz de la confianza. Contiene una única clave PK pública que se utiliza en la cadena de confianza para actualizar la base de datos de claves de intercambio de claves (KEK).

Para cambiar la base de datos de PK, debe tener la clave PK privada para firmar una solicitud de actualización. Esto incluye eliminar la base de datos de PK escribiendo una clave PK vacía.

Base de datos de claves de intercambio de claves (KEK)

La base de datos KEK es una lista de claves KEK públicas que se utilizan en la cadena de confianza para actualizar las bases de datos de firma (db) y de la lista de denegación (dbx).

Para cambiar la base de datos de KEK pública, debe tener la clave PK privada para firmar una solicitud de actualización.

Base de datos de firmas (db)

La base de datos db es una lista de claves públicas y hashes que se utilizan en la cadena de confianza para validar todos los binarios de arranque UEFI.

Para cambiar la base de datos db, debe tener la clave PK privada o cualquiera de las claves KEK privadas para firmar una solicitud de actualización.

Base de datos de la lista de denegación de firmas (dbx)

La base de datos dbx es una lista de claves públicas y hashes binarios que no son de confianza y se utilizan en la cadena de confianza como archivo de revocación.

La base de datos dbx siempre tiene prioridad sobre las demás bases de datos clave.

Para cambiar la base de datos dbx, debe tener la clave PK privada o cualquiera de las claves KEK privadas para firmar una solicitud de actualización.

El Foro UEFI mantiene un dbx disponible de forma pública para muchos binarios y certificados incorrectos en https://uefi.org/revocationlistfile.

Important

UEFI Secure Boot aplica la validación de firmas en cualquier binario UEFI. Para permitir la ejecución de un binario UEFI en el arranque seguro UEFI, debe firmarlo con cualquiera de las claves de base de datos privadas descritas anteriormente.

De forma predeterminada, UEFI Secure Boot está desactivado y el sistema está en `SetupMode`. Cuando el sistema está en `SetupMode`, todas las variables clave se pueden actualizar sin una firma criptográfica. Cuando se establece el PK, el arranque seguro UEFI se habilita y se cierra el modo de configuración.

Lance una instancia con soporte de UEFI Secure Boot

Cuando inicia una instancia con los siguientes requisitos previos, la instancia validará de forma automática los binarios de arranque UEFI en su base de datos UEFI Secure Boot. También puede configurar UEFI Secure Boot en una instancia posterior a al inicialización.

Note

UEFI Secure Boot protege su instancia y su sistema operativo contra las modificaciones del flujo de arranque. Normalmente, UEFI Secure Boot se configura como parte de la AMI. Si crea una nueva AMI con parámetros distintos de la AMI base, como cambiar `UefiData` dentro de la AMI, puede desactivar UEFI Secure Boot.

Requisitos previos

AMI de Linux

Para lanzar una instancia de Linux, la AMI de Linux debe tener habilitado el arranque seguro de la UEFI.

Amazon Linux admite Arranque seguro UEFI a partir de la versión 2023.1 de AL2023. Sin embargo, el arranque seguro UEFI no está habilitado en las AMI predeterminadas. Para obtener más información, consulte Arranque seguro UEFI en la Guía del usuario de AL2023. Las versiones anteriores de las AMI de Amazon Linux no están habilitadas para el arranque seguro UEFI. Para utilizar una AMI admitida, debe realizar varios pasos de configuración en su propia AMI de Linux. Para obtener más información, consulte Crear una AMI de Linux para admitir UEFI Secure Boot.

AMI de Windows

Para lanzar una instancia de Windows, la AMI de Windows debe tener habilitado el arranque seguro de la UEFI.

Las siguientes AMI de Windows están preconfiguradas para habilitar un arranque seguro UEFI con claves de Microsoft:

- TPM-Windows_Server-2022-English-Core-Base
- TPM-Windows_Server-2022-English-Full-Base
- TPM-Windows_Server-2022-English-Full-SQL_2022_Enterprise
- TPM-Windows_Server-2022-English-Full-SQL_2022_Standard
- TPM-Windows_Server-2019-English-Core-Base
- TPM-Windows_Server-2019-English-Full-Base
- TPM-Windows_Server-2019-English-Full-SQL_2019_Enterprise
- TPM-Windows_Server-2019-English-Full-SQL_2019_Standard
- TPM-Windows_Server-2016-English-Core-Base
- TPM-Windows_Server-2016-English-Full-Base

En este momento, no se admite la importación de Windows con UEFI Secure Boot mediante el comando import-image.

Tipo de instancia

- Compatibles: todos los tipos de instancias virtualizadas que admiten UEFI también admiten UEFI Secure Boot. Para obtener información sobre los tipos de instancias compatibles con el modo Arranque seguro UEFI, consulte Consideraciones.
- No compatibles: los tipos de instancias bare metal no admiten UEFI Secure Boot.

Comprobar si una instancia está habilitada para UEFI Secure Boot

instancias de Linux

Puede usar la utilidad `mokutil` para verificar si una instancia de Linux está habilitada para UEFI Secure Boot. Si `mokutil` no está instalado en la instancia, deberá instalarlo. Para obtener las instrucciones de instalación en Amazon Linux 2, consulte https://docs.aws.amazon.com/linux/al2/ug/find-install-software.html. Para otras distribuciones de Linux, consulte su documentación específica.

Para verificar si una instancia de Linux está habilitada para UEFI Secure Boot

Ejecute el siguiente comando como `root` en la instancia.

```
mokutil --sb-state
```

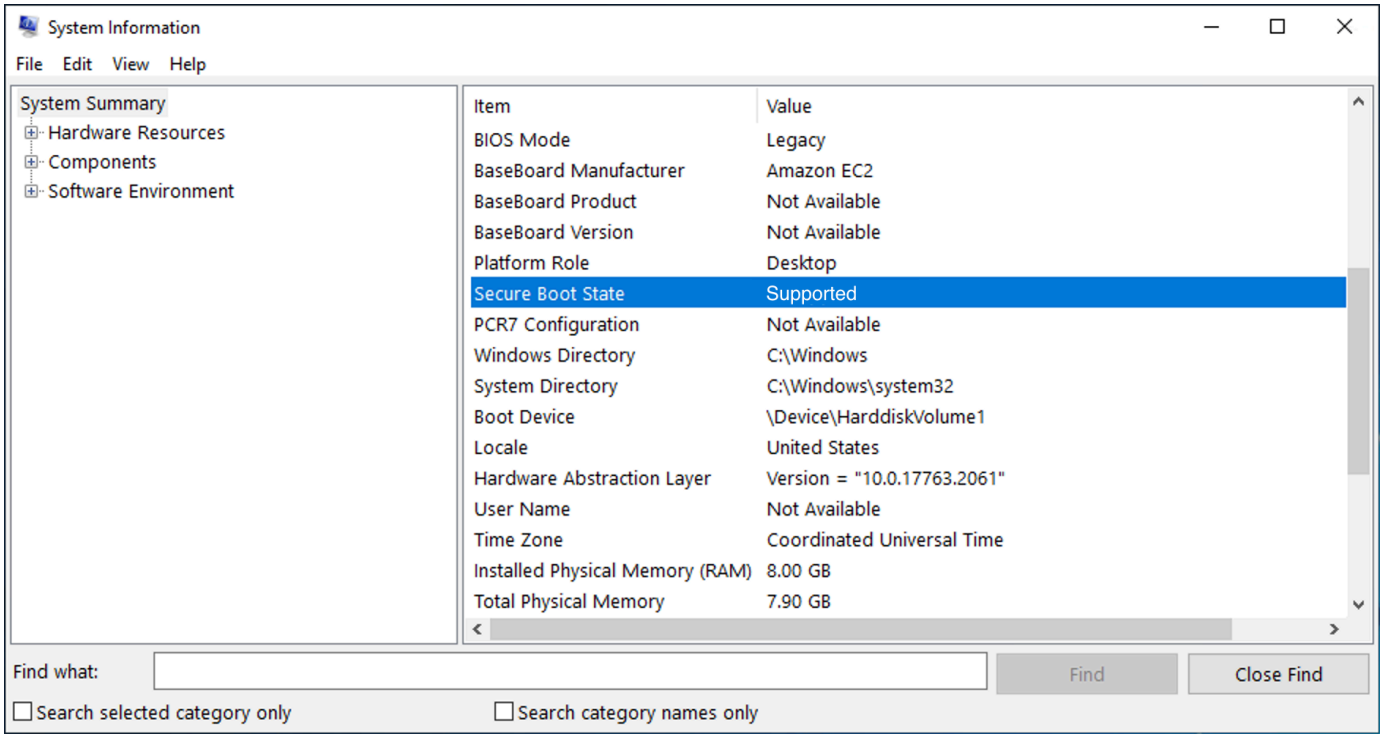
Resultado previsto:

- Si el arranque seguro UEFI está habilitado, la salida contiene `SecureBoot enabled`.
- Si UEFI Secure Boot no está habilitado, la salida contiene `SecureBoot disabled` o `Failed to read SecureBoot`.

instancias de Windows

Para comprobar si una instancia de Windows está habilitada para UEFI Secure Boot

1. Abra la herramienta msinfo32.
2. Verifique el campo Estado de arranque seguro. La opción Compatible indica que el arranque seguro UEFI está habilitado.



También puede utilizar Cmdlet `Confirm-SecureBootUEFI` de Windows PowerShell para verificar el estado de arranque seguro. Para obtener más información sobre el comando cmdlet, consulte Confirm-SecureBootUEFI en el sitio web de documentación de Microsoft.

Crear una AMI de Linux para admitir UEFI Secure Boot

En los siguientes procedimientos, se describe cómo crear un almacenaje de variables UEFI para un arranque seguro con claves privadas personalizadas. Amazon Linux admite Arranque seguro UEFI a partir de la versión 2023.1 de AL2023. Para obtener más información, consulte Arranque seguro UEFI en la Guía del usuario de AL2023.

> **Important**
>
> Los siguientes procedimientos para crear una AMI que sea compatible con el arranque seguro UEFI están dirigidos únicamente a usuarios avanzados. Debe tener el conocimiento suficiente del flujo de arranque de distribución SSL y Linux para utilizar estos procedimientos.

Requisitos previos

- Se utilizarán las siguientes herramientas:

  - OpenSSL: https://www.openssl.org/
  - efivar: https://github.com/rhboot/efivar
  - efitools: https://git.kernel.org/pub/scm/linux/kernel/git/jejb/efitools.git/
  - Comando get-instance-uefi-data de la AWS CLI
- La instancia de Linux debe haberse iniciado con una AMI de Linux compatible con el modo de arranque UEFI y debe tener datos no volátiles presentes.

Las instancias recientemente creadas sin claves de UEFI Secure Boot se crean en `SetupMode`, lo que le permite inscribir claves propias. Algunas AMI vienen preconfiguradas con UEFI Secure Boot y no se pueden cambiar las claves existentes. Si desea cambiar las claves, debe crear una AMI nueva basada en la AMI original.

Existen dos formas de propagar las claves en el almacén de variables, las cuales se describen en la opción A y la opción B que se indican a continuación. En la opción A, se describe cómo hacerlo desde la instancia, imitando el flujo de hardware real. En la opción B, se describe cómo crear un blob binario, que luego se pasa como un archivo codificado en base64 cuando se crea la AMI. Para ambas opciones, primero debe crear los tres pares de claves, que se utilizan para la cadena de confianza.

Para crear una AMI de Linux que admita UEFI Secure Boot, cree primero los tres pares de claves y, a continuación, complete la opción A o la opción B:

- Crear tres pares de claves
- Opción A: agregar claves al almacén de variables desde la instancia
- Opción B: crear un blob binario que contenga un almacén de variables precargado

> **Note**
>
> Estas instrucciones solo se pueden utilizar para crear una AMI de Linux. Si necesita una AMI de Windows, utilice una de las AMI de Windows compatibles. Para obtener más información, consulte Lance una instancia con soporte de UEFI Secure Boot.

Crear tres pares de claves

UEFI Secure Boot se basa en las tres bases de datos clave siguientes, que se utilizan en una cadena de confianza: la clave de plataforma (PK), la clave de intercambio de claves (KEK) y la base de datos de firmas (db).[1]

Cada clave se crea en la instancia. Para preparar las claves públicas en un formato que sea válido para el estándar UEFI Secure Boot, cree un certificado para cada clave. Las `DER` definen el formato SSL (codificación binaria de un formato). A continuación, convierta cada certificado en una lista de firmas UEFI, que es el formato binario que entiende UEFI Secure Boot. Y, por último, firme cada certificado con la clave correspondiente.

Temas

Preparación para la creación de pares de claves

Antes de crear los pares de claves, cree un identificador único global (GUID) que se utilizará en la generación de claves.

1. Conéctese a la instancia.
2. Ejecute el siguiente comando en una línea del shell.

```
uuidgen --random > GUID.txt
```

Par de claves 1: cree la clave de plataforma (PK)

La PK es la raíz de la confianza de las instancias UEFI Secure Boot. La PK privada se utiliza para actualizar la KEK, que, a su vez, se puede utilizar para agregar claves autorizadas a la base de datos de firmas (db).

El estándar X.509 se utiliza para crear el par de claves. Para obtener información sobre el estándar, consulte X.509 en Wikipedia.

Para crear la PK

1. Cree la clave. Debe nombrar la variable PK.

   ```
   openssl req -newkey rsa:4096 -nodes -keyout PK.key -new -x509 -sha256 -days 3650 -
   subj "/CN=Platform key/" -out PK.crt
   ```

   Se especifican los siguientes parámetros:

   - `-keyout PK.key`: el archivo de la clave privada.
   - `-days 3650`: el número de días en que el certificado es válido.
   - `-out PK.crt`: el certificado que se utiliza para crear la variable UEFI.
   - `CN=Platform key`: el nombre común (CN) para la clave. Puede escribir el nombre de su organización en lugar de la *Clave de plataforma*.
2. Cree el certificado.

   ```
   openssl x509 -outform DER -in PK.crt -out PK.cer
   ```
3. Convierta el certificado en una lista de firmas UEFI.

   ```
   cert-to-efi-sig-list -g "$(< GUID.txt)" PK.crt PK.esl
   ```
4. Firme la lista de firmas de la UEFI con la PK privada (autofirmado).

   ```
   sign-efi-sig-list -g "$(< GUID.txt)" -k PK.key -c PK.crt PK PK.esl PK.auth
   ```

Par de claves 2: cree la clave de intercambio de claves (KEK)

La KEK privada se utiliza para agregar claves a la db, que es la lista de firmas autorizadas para arrancar en el sistema.

Para crear la clave de intercambio de claves (KEK)

1. Cree la clave.

   ```
   openssl req -newkey rsa:4096 -nodes -keyout KEK.key -new -x509 -sha256 -days 3650 -
   subj "/CN=Key Exchange Key/" -out KEK.crt
   ```
2. Cree el certificado.

```
openssl x509 -outform DER -in KEK.crt -out KEK.cer
```

3. Convierta el certificado en una lista de firmas UEFI.

```
cert-to-efi-sig-list -g "$(< GUID.txt)" KEK.crt KEK.esl
```

4. Firme la lista de firmas con la PK privada.

```
sign-efi-sig-list -g "$(< GUID.txt)" -k PK.key -c PK.crt KEK KEK.esl KEK.auth
```

Par de claves 3: cree la base de datos (DB) de firmas

La lista de base de datos contiene claves autorizadas para arrancar en el sistema. Para modificar la lista, es necesario la KEK privada. Las imágenes de arranque se firmarán con la clave privada que se crea en este paso.

Para crear la base de datos

1. Cree la clave.

```
openssl req -newkey rsa:4096 -nodes -keyout db.key -new -x509 -sha256 -days 3650 -
subj "/CN=Signature Database key/" -out db.crt
```

2. Cree el certificado.

```
openssl x509 -outform DER -in db.crt -out db.cer
```

3. Convierta el certificado en una lista de firmas UEFI.

```
cert-to-efi-sig-list -g "$(< GUID.txt)" db.crt db.esl
```

4. Firme la lista de firmas con la KEK privada.

```
sign-efi-sig-list -g "$(< GUID.txt)" -k KEK.key -c KEK.crt db db.esl db.auth
```

Firme la imagen de arranque (kernel) con la clave privada

Para Ubuntu 22.04, las siguientes imágenes requieren firmas.

```
/boot/efi/EFI/ubuntu/shimx64.efi
/boot/efi/EFI/ubuntu/mmx64.efi
/boot/efi/EFI/ubuntu/grubx64.efi
/boot/vmlinuz
```

Para firmar una imagen

Utilice la siguiente sintaxis para firmar una imagen.

```
sbsign --key db.key --cert db.crt --output /boot/vmlinuz /boot/vmlinuz
```

> **Note**
>
> Debe firmar todos los nuevos kernels. En general, */boot/vmlinuz* creará un enlace simbólico con el último kernel instalado.

Para obtener más información sobre la cadena de arranque y las imágenes requeridas, consulte la documentación correspondiente para su distribución.

[1] Gracias a la comunidad ArchWiki por todo el trabajo que ha realizado. Los comandos para crear la PK, la KEK, la base de datos, así como también para firmar la imagen provienen de la documentación Creación de claves, redactado por el equipo de mantenimiento de ArchWiki y los colaboradores de ArchWiki.

Opción A: agregar claves al almacén de variables desde la instancia

Una vez que haya creado los tres pares de claves, puede conectar con su instancia y agregar las claves al almacén de variables desde la instancia con los siguientes pasos.

Pasos de la opción A:

- Paso 1: iniciar una instancia que sea compatible con UEFI Secure Boot
- Paso 2: configurar una instancia de forma que admita UEFI Secure Boot
- Paso 3: crear una AMI a partir de la instancia

Paso 1: iniciar una instancia que sea compatible con UEFI Secure Boot

Cuando inicia una instancia con los siguientes requisitos previos, la instancia estará lista para configurarse de forma que admita UEFI Secure Boot. Solo puede habilitar la compatibilidad con UEFI Secure Boot en una instancia durante la inicialización, no puede habilitarlo más adelante.

Requisitos previos

- AMI: la AMI de Linux tiene que ser compatible con el modo de arranque UEFI. Para comprobar que la AMI es compatible con el modo de arranque UEFI, el parámetro del modo de arranque AMI debe ser uefi. Para obtener más información, consulte Determinar el parámetro de modo de arranque de una AMI.

  Tenga en cuenta que AWS solo proporciona AMI de Linux configuradas para admitir UEFI para tipos de instancias basados en Graviton. En este momento, AWS no proporciona AMI de Linux x86_64 compatibles con el modo de arranque UEFI. Puede configurar su propia AMI para que admita el modo de arranque UEFI en todas las arquitecturas. Para configurar su propia AMI para que admita el modo de arranque UEFI, debe seguir varios pasos de configuración en su propia AMI. Para obtener más información, consulte Establezca el modo de arranque de una AMI.
- Tipo de instancia: todos los tipos de instancias virtualizadas que admiten UEFI también admiten UEFI Secure Boot. Los tipos de instancias bare metal no admiten UEFI Secure Boot. Para obtener información sobre los tipos de instancias compatibles con el modo Arranque seguro UEFI, consulte Consideraciones.
- Inicie su instancia después de la inicialización de UEFI Secure Boot. Solo las instancias iniciadas después del 10 de mayo de 2022 (cuando se lanzó UEFI Secure Boot) pueden admitir UEFI Secure Boot.

Después de iniciar la instancia, puede verificar que está lista para configurarse de forma que admita UEFI Secure Boot (en otras palabras, puede proceder al Paso 2) y comprobar si hay datos UEFI presentes. La presencia de datos de la UEFI indica que persisten los datos no volátiles.

Para verificar si la instancia está lista para el paso 2

Utilice el comando get-instance-uefi-data y especifique el ID de la instancia.

```
aws ec2 get-instance-uefi-data --instance-id i-0123456789example
```

La instancia está lista para el paso 2 si los datos UEFI están presentes en la salida. Si la salida está vacía, la instancia no se puede configurar para que admita UEFI Secure Boot. Esto puede suceder

si la instancia se lanzó antes de que la compatibilidad con UEFI Secure Boot estuviera disponible. Lance una nueva instancia e inténtelo de nuevo.

Paso 2: configurar una instancia de forma que admita UEFI Secure Boot

Inscriba los pares de claves en el almacén de variables UEFI en la instancia

> **Warning**
>
> Debe firmar las imágenes de arranque después de inscribir las claves. De lo contrario, no podrá arrancar la instancia.

Después de crear las listas de firmas de la UEFI firmadas (PK, KEK y db), deben estar inscritas en el firmware de la UEFI.

Escribir en la variable PK solo es posible en los siguientes casos:

- Si aún no se ha inscrito ninguna PK, lo que se indica si la variable `SetupMode` es `1`. Compruébelo mediante el siguiente comando. La salida es `1` o `0`.

  ```
  efivar -d -n 8be4df61-93ca-11d2-aa0d-00e098032b8c-SetupMode
  ```

- Si la nueva PK está firmada por la clave privada de la PK existente.

Para inscribir las claves en el almacén de variables UEFI

Los siguientes comandos deben ejecutarse en la instancia.

Si SetupMode está habilitado (el valor es 1), las claves se pueden inscribir mediante los siguientes comandos en la instancia:

```
[ec2-user ~]$ efi-updatevar -f db.auth db
```

```
[ec2-user ~]$ efi-updatevar -f KEK.auth KEK
```

```
[ec2-user ~]$ efi-updatevar -f PK.auth PK
```

Para comprobar que UEFI Secure Boot está habilitado

Para verificar si el arranque seguro UEFI está habilitado, siga los pasos en Comprobar si una instancia está habilitada para UEFI Secure Boot.

Ahora, puede exportar su almacén de variables UEFI con el comando de la CLI get-instance-uefi-data o puede continuar con el siguiente paso y firmar las imágenes de arranque para reiniciar en una instancia habilitada para UEFI Secure Boot.

Paso 3: crear una AMI a partir de la instancia

Para crear una AMI desde la instancia, puede utilizar la consola o el código `CreateImage` de la API, la CLI o el SDK. Para obtener instrucciones sobre cómo utilizar la consola, consulte Creación de una AMI basada en Amazon EBS. Para obtener instrucciones sobre las API, consulte Crear Imagen.

> **Note**
>
> La API `CreateImage` copia de forma automática el almacén de variables UEFI de la instancia en la AMI. La consola usa la API `CreateImage`. Después de iniciar instancias mediante esta AMI, las instancias tendrán el mismo almacén de variables UEFI.

Opción B: crear un blob binario que contenga un almacén de variables precargado

Una vez que haya creado los tres pares de claves, puede crear un blob binario que contenga un almacén de variables precargado y que, a su vez, contenga las claves de UEFI Secure Boot.

> **Warning**
>
> Debe firmar las imágenes de arranque antes de inscribir las claves; de lo contrario, no podrá arrancar la instancia.

Pasos de la opción B:

- Paso 1: crear un almacén de variables nuevo o actualizar uno existente
- Paso 2: cargar el blob binario en la creación de la AMI

Paso 1: crear un almacén de variables nuevo o actualizar uno existente

Puede crear el almacén de variables sin conexión sin una instancia en ejecución mediante la herramienta python-uefivars. La herramienta puede crear un almacén de variables nuevo a partir

de sus claves. El script admite actualmente el formato EDK2, el formato AWS y una representación JSON que es más fácil de editar con herramientas de nivel superior.

Para crear el almacén de variables sin conexión sin una instancia en ejecución

1. Descargue la herramienta en el siguiente enlace.

   ```
   https://github.com/awslabs/python-uefivars
   ```

2. Cree un nuevo almacén de variables desde sus claves con la ejecución del siguiente comando. Esto creará un blob binario codificado en base64 en *your_binary_blob*.bin. La herramienta también admite la actualización de un blob binario a través del parámetro `-I`.

   ```
   ./uefivars.py -i none -o aws -O your_binary_blob.bin -P PK.esl -K KEK.esl --db
    db.esl --dbx dbx.esl
   ```

Paso 2: cargar el blob binario en la creación de la AMI

Utilice register-image para pasar los datos del almacén de variables UEFI. Para el parámetro `--uefi-data`, especifique el blob binario y para el parámetro `--boot-mode`, especifique `uefi`.

```
aws ec2 register-image \
    --name uefi_sb_tpm_register_image_test \
    --uefi-data $(cat your_binary_blob.bin) \
    --block-device-mappings "DeviceName=/dev/sda1,Ebs=
 {SnapshotId=snap-0123456789example,DeleteOnTermination=true}" \
    --architecture x86_64 \
    --root-device-name /dev/sda1 \
    --virtualization-type hvm \
    --ena-support \
    --boot-mode uefi
```

Cómo se crea el blob binario de AWS

Puede seguir los siguientes pasos para personalizar las variables de UEFI Secure Boot durante la creación de AMI. El KEK que se utiliza en estos pasos está actualizado a partir de septiembre de 2021. Si Microsoft actualiza la KEK, debe utilizar la KEK más reciente.

Para crear el blob binario de AWS

1. Cree una lista de firmas de PK vacía.

```
touch empty_key.crt
cert-to-efi-sig-list empty_key.crt PK.esl
```

2. Descargue el certificado KEK.

```
https://go.microsoft.com/fwlink/?LinkId=321185
```

3. Empaque los certificados KEK en una lista de firmas UEFI (`siglist`).

```
sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --output
 MS_Win_KEK.esl MicCorKEKCA2011_2011-06-24.crt
```

4. Descargue los certificados de la db de Microsoft.

```
https://www.microsoft.com/pkiops/certs/MicWinProPCA2011_2011-10-19.crt
https://www.microsoft.com/pkiops/certs/MicCorUEFCA2011_2011-06-27.crt
```

5. Genere la lista de firmas de la db.

```
sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --output
 MS_Win_db.esl MicWinProPCA2011_2011-10-19.crt
sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --output
 MS_UEFI_db.esl MicCorUEFCA2011_2011-06-27.crt
cat MS_Win_db.esl MS_UEFI_db.esl > MS_db.esl
```

6. Descargue una solicitud de cambio dbx actualizada desde el siguiente enlace.

```
https://uefi.org/revocationlistfile
```

7. La solicitud de cambio dbx que descargó en el paso anterior ya está firmada con Microsoft KEK, por lo que debe eliminarla o descomprimirla. Puede utilizar los siguientes enlaces.

```
https://gist.github.com/out0xb2/f8e0bae94214889a89ac67fceb37f8c0
```

```
https://support.microsoft.com/en-us/topic/microsoft-guidance-for-applying-secure-
boot-dbx-update-e3b9e4cb-a330-b3ba-a602-15083965d9ca
```

8. Cree un almacén de variables UEFI utilizando el script `uefivars.py`.

```
./uefivars.py -i none -o aws -O uefiblob-microsoft-keys-empty-pk.bin -P ~/PK.esl -K
 ~/MS_Win_KEK.esl --db ~/MS_db.esl  --dbx ~/dbx-2021-April.bin
```

9. Compruebe el blob binario y el almacén de variables UEFI.

```
./uefivars.py -i aws -I uefiblob-microsoft-keys-empty-pk.bin -o json | less
```

10. Puede actualizar el blob cargándolo nuevamente en la misma herramienta.

```
./uefivars.py -i aws -I uefiblob-microsoft-keys-empty-pk.bin -o aws -O uefiblob-
microsoft-keys-empty-pk.bin -P ~/PK.esl -K ~/MS_Win_KEK.esl --db ~/MS_db.esl  --dbx
 ~/dbx-2021-April.bin
```

    Resultado previsto

```
Replacing PK
Replacing KEK
Replacing db
Replacing dbx
```

Buscar una AMI

Una AMI incluye los componentes y las aplicaciones, como el sistema operativo y el tipo de volumen raíz, necesarios para lanzar una instancia. Para lanzar una instancia que satisfaga sus necesidades, debe buscar una AMI que satisfaga sus necesidades.

Cuando seleccione una AMI, tenga en cuenta los siguientes requisitos que podría tener para las instancias que desea lanzar:

- La región: los ID de AMI son exclusivos para cada región de AWS.
- El sistema operativo
- La arquitectura: 32 bits (`i386`), 64 bits (`x86_64`), ARM 64 bits (`arm64`)
- El tipo de dispositivo raíz: Amazon EBS o almacén de instancias
- El proveedor (por ejemplo, Amazon Web Services)
- Software adicional (por ejemplo, SQL Server)

Existen varias formas de encontrar una AMI que satisfaga sus necesidades. En este tema se describe cómo encontrar una AMI con la consola de Amazon EC2, AWS CLI, AWS Tools for Windows PowerShell y AWS Systems Manager.

Temas

Cómo buscar una AMI de mediante la consola de Amazon EC2

Puede encontrar AMI mediante la consola de Amazon EC2. Puede seleccionar en la lista de AMI cuando utilice el asistente de inicialización de instancias para iniciar una instancia, o bien puede buscar en todas las AMI disponibles mediante la página Imágenes.

Para buscar una AMI mediante el asistente de inicialización de instancias

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la barra de navegación, seleccione la región en la que se iniciarán las instancias. Puede seleccionar cualquier región disponible, independientemente de su ubicación. Cada ID de AMI es exclusivo para cada región de AWS.
3. En el panel de la consola, elija Iniciar instancia.
4. (Nueva consola) En Imágenes de aplicaciones y sistema operativo (imagen de máquina de Amazon), elija Inicio rápido, elija el sistema operativo de la instancia y, a continuación, en Imagen de máquina de Amazon (AMI), seleccione una de las AMI más utilizadas que aparecen en la lista. Si no ve la AMI que necesita, puede elegir Examinar más AMI para navegar por el catálogo completo de AMI. Para obtener más información, consulte Imágenes de aplicaciones y sistema operativo (Imagen de máquina de Amazon).

   (Consola antigua) En la pestaña Inicio rápido, seleccione una de las AMI más utilizadas que aparecen en la lista. Si no ve la AMI que desea utilizar, elija la pestaña Mi AMI, AWS Marketplace o AMI de la comunidad para buscar AMI adicionales. Para obtener más información, consulte Paso 1: Elegir una Imagen de máquina de Amazon (AMI).

Para buscar una AMI mediante la página de AMI

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la barra de navegación, seleccione la región en la que se iniciarán las instancias. Puede seleccionar cualquier región disponible, independientemente de su ubicación. Cada ID de AMI es exclusivo para cada región de AWS.
3. En el panel de navegación, elija AMI.
4. (Opcional) Utilice las opciones Filtrar y Buscar para acotar la lista de AMI que se muestran de modo que solo aparezcan las AMI que coincidan con sus criterios.

   Por ejemplo, para enumerar todas las AMI que proporciona AWS, seleccione Imágenes públicas. Después, utilice las opciones de búsqueda para acotar aún más la lista de AMI mostradas. Elija la barra Buscar y, en el menú, elija Alias del propietario, luego el operador = y luego el valor amazon. Para buscar las AMI que coincidan con una plataforma específica, por ejemplo, Linux o Windows, vuelva a seleccionar la barra de búsqueda para elegir Plataforma, luego el operador = y, por último, el sistema operativo de la lista proporcionada.
5. (Opcional) Elija el icono Preferencias para seleccionar los atributos de imagen que se van a mostrar, como el tipo de dispositivo raíz. Además, puede seleccionar una AMI de la lista y ver sus propiedades en la pestaña Detalles.
6. Antes de seleccionar una AMI, es importante que compruebe si está respaldada por un almacén de instancias o por Amazon EBS, y que usted es consciente de los efectos de esta diferencia. Para obtener más información, consulte Almacenamiento para el dispositivo raíz.
7. Para iniciar una instancia desde esta AMI, selecciónela y elija iniciar instancia a partir de una imagen. Para obtener información sobre el uso de la consola para iniciar una instancia, consulte Lance una instancia con el nuevo asistente de inicialización de instancias. Si no está preparado para iniciar la instancia en ese momento, anote el ID de la AMI para usarlo más adelante.

Buscar una AMI mediante el AWS CLI

Puede usar el comando de la AWS CLI describe-images para obtener una lista solo de las AMI que satisfagan sus necesidades. Una vez que haya encontrado una AMI que coincida con sus requisitos, anote su ID para poder utilizarla para iniciar instancias. Para obtener más información, consulte iniciar la instancia en la Guía del usuario de AWS Command Line Interface.

El comando describe-images admite parámetros de filtrado. Por ejemplo, utilice el parámetro `--owners` para mostrar las AMI públicas propiedad de Amazon.

```
aws ec2 describe-images --owners amazon
```

Puede agregar el siguiente filtro al comando anterior para mostrar solo las AMI de Windows.

```
--filters "Name=platform,Values=windows"
```

Puede añadir el siguiente filtro al comando anterior para mostrar solo las AMI con respaldo Amazon EBS.

```
--filters "Name=root-device-type,Values=ebs"
```

> **Important**
>
> La omisión del parámetro `--owners` del comando `describe-images` devuelve todas las imágenes para las que tiene permisos de inicialización, independientemente de quién sea su propietario.

Buscar una AMI mediante el AWS Tools for Windows PowerShell

Puede utilizar cmdlets de PowerShell para obtener una lista que contenga solo las AMI de Windows que coincidan con sus requisitos. Para obtener más información y ejemplos, consulte Buscar una Amazon Machine Image mediante Windows PowerShell en la Guía del usuario de AWS Tools for Windows PowerShell.

Una vez que haya encontrado una AMI que coincida con sus requisitos, anote su ID para poder utilizarla para iniciar instancias. Para obtener más información, consulte Inicialización de una instancia de Amazon EC2 mediante Windows PowerShell en la Guía del usuario de AWS Tools for Windows PowerShell.

Cómo buscar una AMI con un parámetro de Systems Manager

Cuando inicia una instancia con el asistente de inicialización de instancias EC2 en la consola de Amazon EC2, puede seleccionar una AMI de la lista (según se describe en Cómo buscar una AMI de mediante la consola de Amazon EC2) o seleccionar un parámetro AWS Systems Manager que apunte a un ID de AMI (según se describe en esta sección). Si utiliza código de automatización para iniciar las instancias, puede especificar el parámetro de Systems Manager en lugar del ID de AMI.

Un parámetro de Systems Manager es un par clave-valor definido por el cliente que puede crear en el almacén de parámetros de Systems Manager. El almacén de parámetros proporciona un almacén central para externalizar los valores de configuración de la aplicación. Para obtener más información, consulte el Almacén de parámetros de AWS Systems Manager en la Guía del usuario de AWS Systems Manager.

Cuando cree un parámetro que apunte a un ID de AMI, asegúrese de especificar el tipo de datos como `aws:ec2:image`. Especificar este tipo de datos garantiza que, cuando se crea o modifica el parámetro, el valor del parámetro se valida como un ID de AMI. Para obtener más información, consulte Compatibilidad con parámetros nativos para los ID de Imagen de máquina de Amazon en la Guía del usuario de AWS Systems Manager.

Temas

Casos de uso

Cuando utiliza los parámetros de Systems Manager para apuntar a los ID de AMI, es más fácil para los usuarios seleccionar la AMI correcta cuando inician las instancias. Los parámetros de Systems Manager también pueden simplificar el mantenimiento del código de automatización.

Más fácil para los usuarios

Si necesita que las instancias se lancen con una AMI específica y si esa AMI se actualiza con regularidad, se recomienda que exija a los usuarios que seleccionen un parámetro de Systems Manager para encontrar la AMI. Exigir a los usuarios que seleccionen un parámetro de Systems Manager garantiza que se utilice la última AMI para iniciar instancias.

Por ejemplo, cada mes en su organización puede crear una nueva versión de su AMI que tenga los últimos parches de aplicaciones y sistema operativo. También requiere que los usuarios inicien instancias con la última versión de su AMI. Para asegurarse de que los usuarios utilizan la versión más reciente, puede crear un parámetro de Administrador de sistemas (por ejemplo, `golden-ami`) que apunte al ID de AMI correcto. Cada vez que se crea una nueva versión de la AMI, se actualiza el valor del ID de la AMI en el parámetro para que siempre apunte a la AMI más reciente. No es necesario que los usuarios sepan sobre las actualizaciones periódicas de la AMI, ya que seleccionan

el mismo parámetro de Systems Manager cada vez. Utilizar un parámetro de Systems Manager para su AMI les facilita seleccionar la AMI correcta para la inicialización de una instancia.

Simplificar el mantenimiento del código de automatización

Si utiliza código de automatización para iniciar las instancias, puede especificar el parámetro de Systems Manager en lugar del ID de AMI. Si se crea una versión nueva de la AMI, puede cambiar el valor del ID de la AMI en el parámetro para que apunte a la AMI más reciente. Cada vez que se crea una nueva versión de la AMI no tiene que modificarse el código de automatización que hace referencia al parámetro. Esto simplifica el mantenimiento de la automatización y ayuda a reducir los costos de implementación.

> **Note**
>
> Las instancias en ejecución no se ven afectadas cuando se cambia el ID de la AMI al que apunta el parámetro de Systems Manager.

Permisos

Si utiliza parámetros de Systems Manager que apuntan a los ID de AMI en el asistente de inicialización de instancias, debe agregar los siguientes permisos a la política de IAM:

- `ssm:DescribeParameters`: concede permiso para ver y seleccionar parámetros de Systems Manager.
- `ssm:GetParameters`: concede permiso para recuperar los valores de los parámetros de Systems Manager.

También puede restringir el acceso a parámetros de Systems Manager específicos. Para obtener más información y políticas de IAM de ejemplo, consulte Ejemplo: uso del asistente de inicialización de instancias de EC2.

Limitaciones

Las AMI y los parámetros de Systems Manager son específicos de la región. Para utilizar el mismo nombre de parámetro de Administrador de sistemas en regiones, cree un parámetro de Administrador de sistemas en cada región con el mismo nombre (por ejemplo, `golden-ami`). En cada región, apunte con el parámetro de Systems Manager a una AMI de esa región.

Iniciar una instancia mediante un parámetro de Systems Manager

Puede iniciar una instancia usando la consola o la AWS CLI. En lugar de especificar un ID de AMI, puede especificar un parámetro de AWS Systems Manager que apunte a un ID de AMI.

New console

Para buscar una AMI mediante un parámetro de Systems Manager (consola)

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la barra de navegación, seleccione la región en la que se iniciarán las instancias. Puede seleccionar cualquier región disponible, independientemente de su ubicación.
3. En el panel de la consola, elija Launch Instance (Iniciar instancia).
4. En (Imágenes de aplicaciones y sistema operativo (imagen de máquina de Amazon), elija Buscar más AMI.
5. Elija el botón de flecha situado a la derecha de la barra de búsqueda y luego elija Buscar por parámetro de Systems Manager.
6. Para Parámetro de Systems Manager, seleccione un parámetro. El ID de AMI correspondiente aparece junto a Actualmente se resuelve en.
7. Elija Buscar. Las AMI que coinciden con el ID de AMI aparecen en la lista.
8. Seleccione la AMI de la lista y elija Seleccionar.

Para obtener más información sobre cómo iniciar una instancia con el asistente de inicialización de instancias, consulte Lance una instancia con el nuevo asistente de inicialización de instancias.

Old console

Para buscar una AMI mediante un parámetro de Systems Manager (consola)

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la barra de navegación, seleccione la región en la que se iniciarán las instancias. Puede seleccionar cualquier región disponible, independientemente de su ubicación.
3. En el panel de la consola, elija Launch Instance (Iniciar instancia).
4. Elija Buscar por parámetro de Administrador de sistemas (en la parte superior derecha).
5. Para Systems Manager parameter (Parámetro de Systems Manager), seleccione un parámetro. El ID de AMI correspondiente aparece junto a Actualmente se resuelve en.

6. Elija Search (Buscar). Las AMI que coinciden con el ID de AMI aparecen en la lista.
7. Seleccione la AMI de la lista y elija Seleccionar.

   Para obtener más información sobre cómo iniciar una instancia desde una AMI con el asistente de inicialización de instancias, consulte Paso 1: Elegir una Imagen de máquina de Amazon (AMI).

Para iniciar una instancia utilizando un parámetro de AWS Systems Manager en lugar de un ID de AMI (AWS CLI)

En el ejemplo siguiente se utiliza el parámetro de Administrador de sistemas `golden-ami` para iniciar una instancia `m5.xlarge`. El parámetro apunta a un ID de AMI.

Para especificar el parámetro en el comando, utilice la siguiente sintaxis: `resolve:ssm:/parameter-name`, donde `resolve:ssm` es el prefijo estándar y `parameter-name` es el nombre de parámetro único. Tenga en cuenta que el nombre de parámetro distingue entre mayúsculas y minúsculas. Las barras diagonales inversas para el nombre del parámetro solo son necesarias cuando el parámetro forma parte de una jerarquía, por ejemplo, `/amis/production/golden-ami`. Puede omitir la barra invertida si el parámetro no forma parte de una jerarquía.

En el ejemplo, los parámetros `--count` y `--security-group` no están incluidos. En el caso de `--count`, el valor predeterminado es 1. Si tiene una VPC predeterminada y un grupo de seguridad predeterminado, estos serán los que se utilicen.

```
aws ec2 run-instances
    --image-id resolve:ssm:/golden-ami
    --instance-type m5.xlarge
    ...
```

Para iniciar una instancia usando una versión específica de un parámetro de AWS Systems Manager (AWS CLI)

Los parámetros de Systems Manager tienen compatibilidad de versión. A cada iteración de un parámetro se le asigna un número de versión único. Puede hacer referencia a la versión del parámetro de la siguiente manera: `resolve:ssm:parameter-name:version`, donde `version` es el número de versión único. De forma predeterminada, se utiliza la última versión del parámetro cuando no se especifica ninguna versión.

En el ejemplo siguiente se utiliza la versión 2 del parámetro.

En el ejemplo, los parámetros `--count` y `--security-group` no están incluidos. Para `--count`, el valor predeterminado es 1. Si tiene una VPC predeterminada y un grupo de seguridad predeterminado, estos serán los que se utilicen.

```
aws ec2 run-instances
    --image-id resolve:ssm:/golden-ami:2
    --instance-type m5.xlarge
    ...
```

Para iniciar una instancia con un parámetro público proporcionado por AWS

Systems Manager proporciona parámetros públicos para las AMI públicas que proporciona AWS. Puede utilizar los parámetros públicos al lanzar instancias para asegurarse de que utiliza las AMI más recientes.

Para obtener más información, consulte Cómo buscar las AMI más recientes mediante Systems Manager.

Cómo buscar las AMI más recientes mediante Systems Manager

AWS Systems Manager proporciona parámetros públicos para las AMI públicas mantenidas por AWS. Puede utilizar los parámetros públicos al lanzar instancias para asegurarse de que utiliza las AMI más recientes. Por ejemplo, el parámetro público `/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-default-arm64` está disponible en todas las regiones y siempre apunta a la versión más reciente de la AMI Amazon Linux 2023 para la arquitectura arm64 en una región determinada.

Los parámetros públicos están disponibles en las siguientes rutas:

- Linux: `/aws/service/ami-amazon-linux-latest`
- Windows: `/aws/service/ami-windows-latest`

Para ver una lista de todas las AMI de Linux o Windows de la región AWS actual

Utilice el siguiente comando de la AWS CLI get-parameters-by-path para ver una lista de todas las AMI de Linux o Windows de la región AWS actual. El valor del parámetro `--path` es diferente para Linux y Windows.

Para Linux:

```
aws ssm get-parameters-by-path \
    --path /aws/service/ami-amazon-linux-latest \
    --query "Parameters[].Name"
```

Para Windows:

```
aws ssm get-parameters-by-path \
    --path /aws/service/ami-windows-latest \
    --query "Parameters[].Name"
```

Para iniciar una instancia con un parámetro público

En el ejemplo siguiente se utiliza el parámetro público de Systems Manager para el ID de imagen a fin de iniciar una instancia con la AMI de Amazon Linux 2023 más reciente.

Para especificar el parámetro en el comando, utilice la siguiente sintaxis: `resolve:ssm:`*`public-parameter`*, donde `resolve:ssm` es el prefijo estándar y *`public-parameter`* es la ruta y el nombre del parámetro público.

En el ejemplo, los parámetros `--count` y `--security-group` no están incluidos. En el caso de `--count`, el valor predeterminado es 1. Si tiene una VPC predeterminada y un grupo de seguridad predeterminado, estos serán los que se utilicen.

```
aws ec2 run-instances \
    --image-id resolve:ssm:/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-default-x86_64 \
    --instance-type m5.xlarge \
    --key-name MyKeyPair
```

Para obtener más información, consulte Trabajar con parámetros públicos en la Guía del usuario de AWS Systems Manager.

Para obtener ejemplos de parámetros de Systems Manager, consulte Consulta de los últimos ID de AMI de Amazon Linux mediante el Almacén de parámetros de AWS Systems Manager y Consulta de las últimas AMI de Windows mediante el Almacén de parámetros de AWS Systems Manager.

Más información para encontrar las AMI

Para encontrar una AMI de Amazon Linux 2023, consulte AL2023 en Amazon EC2 en la Guía del usuario de Amazon Linux 2023.

Para encontrar una AMI de Ubuntu, consulte el Localizador de AMI de Amazon EC2 en el sitio web de Canonical Ubuntu.

Para encontrar una AMI de RHEL, consulte Imágenes de Red Hat Enterprise Linux (AMI) disponibles en Amazon Web Services (AWS) en el sitio web de Red Hat.

AMI compartidas

Una AMI compartida es una AMI que un desarrollador ha creado y puesto a disposición de otros desarrolladores. Una de las formas más sencillas de iniciarse con Amazon EC2 es utilizar una AMI compartida que tenga los componentes que necesita y, a continuación, añadir contenido personalizado. También puede crear sus propias AMI y compartirlas con otros.

El uso de una AMI compartida es por su cuenta y riesgo. Amazon no responde de la integridad o la seguridad de las AMI compartidas por otros usuarios de Amazon EC2. Por lo tanto, debe tratar las AMI compartidas como trataría cualquier código ajeno que desee implementar en su propio centro de datos y ejercer la diligencia debida apropiada. Le recomendamos que las AMI provengan de fuentes de confianza, como un proveedor verificado.

Proveedor verificado

En la consola de Amazon EC2, las AMI públicas que son propiedad de Amazon o de un socio verificado están marcadas con la inscripción Proveedor verificado.

También puede utilizar el comando describe-images de la AWS CLI para identificar las AMI públicas que provienen de un proveedor verificado. Las imágenes públicas de Amazon o de sus socios verificados tienen un propietario con alias, que puede ser `amazon` o `aws-marketplace`. En el resultado de la CLI, estos valores aparecen para `ImageOwnerAlias`. Otros usuarios no pueden asociar las AMI. Esto le permite encontrar las AMI de Amazon o de los socios verificados fácilmente.

Para convertirse en un proveedor verificado, debe registrarse como vendedor en AWS Marketplace. Una vez registrado, puede incluir su AMI en AWS Marketplace. Para obtener más información, consulte Introducción a los vendedores y Productos basados en AMI en la Guía del vendedor de AWS Marketplace.

Temas de AMI compartidas

- Buscar AMI compartidas
- Convertir una AMI en pública

- Compartir una AMI con organizaciones o unidades organizativas específicas
- Compartir una AMI con cuentas de AWS específicas
- Cancelar que se comparta una AMI con su Cuenta de AWS
- Usar marcadores
- Directrices para AMI de Linux compartidas

Si quiere obtener información sobre otros temas

- Para obtener información acerca de la creación de una AMI, consulte the section called “Crear una AMI de Linux con respaldo en el almacén de instancias” o the section called “Creación de una AMI basada en Amazon EBS”.
- Para obtener más información sobre cómo crear, entregar y mantener las aplicaciones en AWS Marketplace, consulte la documentación de AWS Marketplace.

Buscar AMI compartidas

Puede ejecutar consola de Amazon EC2 o la línea de comandos para encontrar AMI compartidas.

Las AMI son un recurso regional. Por tanto, si busca una AMI compartida (pública o privada), debe buscarla en la misma región en la que se está compartiendo. Para hacer que una AMI esté disponible en una región distinta, copie la AMI en dicha región y, a continuación, compártala. Para obtener más información, consulte Copiar una AMI.

Tareas

- Buscar una AMI compartida (consola)
- Buscar una AMI compartida (AWS CLI)
- Buscar una AMI compartida (Tools for Windows PowerShell)
- Usar AMI compartidas

Buscar una AMI compartida (consola)

Para encontrar una AMI privada compartida a través de la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija AMIs.

3. En el primer filtro, elija Imágenes privadas. Se muestran todas las AMI que se han compartido con usted. Para detallar la búsqueda, elija la barra Buscar y utilice las opciones de filtrado del menú.

Para encontrar una AMI pública compartida a través de la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija AMIs.
3. En el primer filtro, elija Imágenes públicas. Para detallar la búsqueda, elija el campo Buscar y utilice las opciones de filtrado del menú.

Encontrar una AMI pública compartida de Amazon a través de la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija AMIs.
3. En el primer filtro, elija Imágenes públicas.
4. Elija el campo Búsqueda y, a continuación, en las opciones de menú que aparecen, seleccione Alias de propietario, luego = y, por último, Amazon para mostrar solo las imágenes públicas de Amazon.

Encontrar una AMI pública compartida de un proveedor verificado a través de la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Catálogo de AMI.
3. Elija AMI de comunidad.
4. La etiqueta Proveedor verificado indica las AMI que son de Amazon o de un socio verificado.

Buscar una AMI compartida (AWS CLI)

Utilice el comando describe-images (AWS CLI) para mostrar una lista de las AMI. Puede limitar la lista según los tipos de AMI que le interesen, tal y como se muestra en los siguientes ejemplos:

Ejemplo: Mostrar todas las AMI públicas

El siguiente comando muestra todas las AMI públicas, incluidas aquellas de su propiedad.

```
aws ec2 describe-images --executable-users all
```

Ejemplo: Mostrar las AMI con permisos de inicialización explícitos

El siguiente comando muestra las AMI para las que tiene permisos de inicialización explícitos. Esta lista no incluye las AMI de su propiedad.

```
aws ec2 describe-images --executable-users self
```

Ejemplo: mostrar las AMI propiedad de proveedores verificados

El siguiente comando muestra las AMI propiedad de los proveedores verificados. Las AMI públicas de proveedores verificados (Amazon o socios verificados) tienen un propietario con alias, el cual aparece como `amazon` o `aws-marketplace` en el campo de cuenta. Esto le permite encontrar AMI de proveedores verificados fácilmente. Otros usuarios no pueden asociar las AMI.

```
aws ec2 describe-images \
    --owners amazon aws-marketplace \
    --query 'Images[*].[ImageId]' \
    --output text
```

Ejemplo: Mostrar las AMI propiedad de una cuenta

El siguiente comando muestra las AMI que son propiedad de la Cuenta de AWS especificada.

```
aws ec2 describe-images --owners 123456789012
```

Ejemplo: Limitar las AMI mediante un filtro

Para reducir el número de AMI que se muestran, utilice un filtro para mostrar solo los tipos de AMI que le interesen. Por ejemplo, utilice el siguiente filtro para mostrar solo las AMI respaldadas por EBS.

```
--filters "Name=root-device-type,Values=ebs"
```

Buscar una AMI compartida (Tools for Windows PowerShell)

Utilice el comando Get-EC2Image (Herramientas para Windows PowerShell) para mostrar una lista de las AMI. Puede limitar la lista según los tipos de AMI que le interesen, tal y como se muestra en los siguientes ejemplos:

Ejemplo: Mostrar todas las AMI públicas

El siguiente comando muestra todas las AMI públicas, incluidas aquellas de su propiedad.

```
PS C:\> Get-EC2Image -ExecutableUser all
```

Ejemplo: Mostrar las AMI con permisos de inicialización explícitos

El siguiente comando muestra las AMI para las que tiene permisos de inicialización explícitos. Esta lista no incluye las AMI de su propiedad.

```
PS C:\> Get-EC2Image -ExecutableUser self
```

Ejemplo: mostrar las AMI propiedad de proveedores verificados

El siguiente comando muestra las AMI propiedad de los proveedores verificados. Las AMI públicas de proveedores verificados (Amazon o socios verificados) tienen un propietario con alias, el cual aparece como `amazon` o `aws-marketplace` en el campo de cuenta. Esto le permite encontrar AMI de proveedores verificados fácilmente. Otros usuarios no pueden asociar las AMI.

```
PS C:\> Get-EC2Image -Owner amazon aws-marketplace
```

Ejemplo: Mostrar las AMI propiedad de una cuenta

El siguiente comando muestra las AMI que son propiedad de la Cuenta de AWS especificada.

```
PS C:\> Get-EC2Image -Owner 123456789012
```

Ejemplo: Limitar las AMI mediante un filtro

Para reducir el número de AMI que se muestran, utilice un filtro para mostrar solo los tipos de AMI que le interesen. Por ejemplo, utilice el siguiente filtro para mostrar solo las AMI respaldadas por EBS.

```
-Filter @{ Name="root-device-type"; Values="ebs" }
```

Usar AMI compartidas

Antes de usar una AMI compartida, siga estos pasos para confirmar que no hay credenciales preinstaladas que pudieran permitir un acceso no deseado a la instancia por parte de terceros

ni registros remotos preconfigurados que pudieran transmitir información confidencial a terceros. Consulte la documentación de la distribución de Linux utilizada por la AMI para obtener información sobre cómo mejorar la seguridad del sistema.

Para garantizar que no pierda acceso a la instancia de manera accidental, le recomendamos que inicie dos sesiones de SSH y que mantenga la segunda de ellas abierta hasta que haya eliminado las credenciales que no reconozca y comprobado que sigue pudiendo iniciar sesión en la instancia a través de SSH.

1. Identificación y deshabilitación de claves SSH públicas no autorizadas. La única clave del archivo debería ser la que usó para iniciar la AMI. El siguiente comando localiza los archivos `authorized_keys`:

   ```
   [ec2-user ~]$ sudo find / -name "authorized_keys" -print -exec cat {} \;
   ```

2. Deshabilitación de autenticación mediante contraseña para el usuario raíz. Abra el archivo `sshd_config` y edite la línea `PermitRootLogin` del modo siguiente:

   ```
   PermitRootLogin without-password
   ```

   También puede deshabilitar la opción iniciar sesión en la instancia como el usuario raíz:

   ```
   PermitRootLogin No
   ```

   Reinicie el servicio sshd.

3. Verifique si existe algún otro usuario que pueda iniciar sesión en la instancia. Los usuarios con privilegios de superusuario son particularmente peligrosos. Elimine o bloquee la contraseña de cualquier cuenta desconocida.
4. Verifique si hay puertos abiertos que no esté utilizando y servicios de red en ejecución que escuchen conexiones entrantes.
5. Para evitar registros remotos preconfigurados, debe eliminar el archivo de configuración existente y reiniciar el servicio `rsyslog`. Por ejemplo:

   ```
   [ec2-user ~]$ sudo rm /etc/rsyslog.conf
   [ec2-user ~]$ sudo service rsyslog restart
   ```

6. Verifique que todos los trabajos cron son legítimos.

Si descubre una AMI pública que considere que podría suponer un riesgo para la seguridad, contacte con el equipo de seguridad de AWS. Para obtener más información, consulte el Centro de seguridad de AWS.

Convertir una AMI en pública

Puede hacer que su AMI esté disponible públicamente y compartirla con todas las Cuentas de AWS.

Si desea impedir que sus AMI se compartan públicamente, habilite el bloqueo del acceso público de las AMI. Esto bloquea cualquier intento de hacer pública una AMI, lo que ayuda a prevenir el acceso no autorizado y el posible uso indebido de los datos de la AMI. Tenga en cuenta que la habilitación del bloqueo del acceso público no afecta a las AMI que ya están disponibles públicamente y que permanecerán en ese estado.

Para permitir que solo cuentas específicas utilicen su AMI para iniciar instancias, consulte Compartir una AMI con cuentas de AWS específicas.

Contenido

Consideraciones

Tenga en cuenta lo siguiente antes de hacer pública una AMI.

- Propiedad: para hacer pública una AMI, su Cuenta de AWS debe ser la propietaria de esta.
- Región: las AMI son un recurso regional. Cuando comparte una AMI, solo está disponible en la región desde donde la compartió. Para hacer que una AMI esté disponible en una región distinta, copie la AMI en dicha región y, a continuación, compártala. Para obtener más información, consulte Copiar una AMI.
- bloqueo del acceso público: para compartir públicamente una AMI, debe deshabilitar el bloqueo del acceso público de las AMI en cada región en la que la AMI se compartirá públicamente. Una vez que haya compartido la AMI públicamente, puede volver a habilitar el bloqueo del acceso público de las AMI para evitar que se sigan compartiendo públicamente.
- Algunas AMI no se pueden hacer públicas: si su AMI tiene alguno de los siguientes componentes, no puede hacerla pública (pero puede compartir la AMI con Cuentas de AWS específicas):

  - Volúmenes cifrados
  - Instantáneas de volúmenes cifrados
  - Códigos de producto
- Evite exponer información confidencial: para evitar exponer información confidencial al compartir una AMI, lea las consideraciones de seguridad disponibles en Directrices para AMI de Linux compartidas y realice las acciones recomendadas.
- Uso: cuando comparte una AMI, los usuarios solo pueden iniciar instancias desde la AMI. No pueden eliminarla, compartirla ni modificarla. Sin embargo, después de iniciar una instancia mediante la AMI, pueden crear una AMI a partir de esa instancia.
- Obsolescencia automática: de forma predeterminada, la fecha de obsolescencia de todas las AMI públicas se establece en dos años a partir de la fecha de creación de la AMI. Puede establecer una fecha de obsolescencia anterior a los dos años. Para anular la fecha de obsolescencia o para aplazarla, debe hacer que la AMI sea privada. Para ello, compártala solo con Cuentas de AWS específicas.
- Eliminar las AMI obsoletas: cuando una AMI pública alcanza su fecha de caducidad, si no se han inicializado instancias nuevas desde la AMI durante seis meses o más, AWS elimina con el tiempo la propiedad de uso compartido público para que las AMI obsoletas no aparezcan en las listas de AMI públicas.
- Facturación: no se factura cuando otras Cuentas de AWS utilizan la AMI para iniciar instancias. Las cuentas que inician instancias mediante la AMI serán facturadas por las instancias iniciadas.

Compartir una AMI con todas las cuentas de AWS (compartir públicamente)

Después de hacer pública una AMI, estará disponible en AMI de la comunidad de la consola, a las que puede acceder desde el Catálogo de AMI en el navegador izquierdo de la consola de EC2 o cuando lance una instancia con la consola. Tenga en cuenta que pueden transcurrir unos minutos antes de que la AMI aparezca en AMI de comunidad una vez que se ha hecho pública.

Console

Para hacer una AMI pública

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione AMIs.
3. Seleccione la AMI de la lista y, a continuación, elija Acciones, Editar permisos de la AMI.

4. En Disponibilidad de AMI, elija Pública.
5. Elija Guardar cambios.

AWS CLI

Cada AMI tiene una propiedad `launchPermission` que controla qué Cuentas de AWS, además de la del propietario, pueden utilizar dicha AMI para iniciar instancias. Al modificar la propiedad `launchPermission` de una AMI, puede hacerla pública (lo cual concede permisos de inicialización a todas las Cuentas de AWS) o compartirla solo con aquellas Cuentas de AWS que especifique.

Puede añadir o eliminar ID de cuentas en la lista de cuentas que tienen permisos de inicialización para una AMI. Para hacer la AMI pública, especifique el grupo `all`. Puede especificar permisos de inicialización públicos y explícitos.

Para hacer una AMI pública

1. Utilice el comando modify-image-attribute del modo siguiente para agregar el grupo `all` a la lista `launchPermission` de la AMI especificada.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission "Add=[{Group=all}]"
```

2. Para verificar los permisos de inicialización de la AMI, utilice el comando describe-image-attribute.

```
aws ec2 describe-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --attribute launchPermission
```

3. (Opcional) Para hacer la AMI privada de nuevo, elimine el grupo `all` de sus permisos de inicialización. Tenga en cuenta que el propietario de la AMI siempre tiene permisos de inicialización, por lo que este comando no le afecta.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission "Remove=[{Group=all}]"
```

PowerShell

Cada AMI tiene una propiedad `launchPermission` que controla qué Cuentas de AWS, además de la del propietario, pueden utilizar dicha AMI para iniciar instancias. Al modificar la propiedad `launchPermission` de una AMI, puede hacerla pública (lo cual concede permisos de inicialización a todas las Cuentas de AWS) o compartirla solo con aquellas Cuentas de AWS que especifique.

Puede añadir o eliminar ID de cuentas en la lista de cuentas que tienen permisos de inicialización para una AMI. Para hacer la AMI pública, especifique el grupo `all`. Puede especificar permisos de inicialización públicos y explícitos.

Para hacer una AMI pública

1. Utilice el comando Edit-EC2ImageAttribute del modo siguiente para agregar el grupo `all` a la lista `launchPermission` de la AMI especificada.

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute
 launchPermission -OperationType add -UserGroup all
```

2. Para verificar los permisos de inicialización de la AMI, utilice el comando Get-EC2ImageAttribute.

```
PS C:\> Get-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute
 launchPermission
```

3. (Opcional) Para hacer la AMI privada de nuevo, elimine el grupo `all` de sus permisos de inicialización. Tenga en cuenta que el propietario de la AMI siempre tiene permisos de inicialización, por lo que este comando no le afecta.

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute
 launchPermission -OperationType remove -UserGroup all
```

bloquee el acceso público de sus AMI

Para impedir que sus AMI se compartan públicamente, habilite el bloqueo del acceso público de las AMI. Esta configuración está habilitada a nivel de cuenta, pero debe habilitarla en cada una de las Región de AWS en las que desee impedir que sus AMI se compartan públicamente.

Cuando el bloqueo del acceso público se habilita, cualquier intento de hacer pública una AMI se bloquea de manera automática. Sin embargo, si ya tiene AMI públicas, permanecerán disponibles públicamente.

Si quiere compartir públicamente las AMI, deberá deshabilitar el bloqueo del acceso público. Cuando haya terminado de compartir, se recomienda volver a habilitar el bloqueo del acceso público para evitar que sus AMI se compartan públicamente sin su consentimiento.

Puede restringir los permisos de IAM a un usuario administrador para que solo esa persona pueda habilitar o deshabilitar el bloqueo del acceso público de las AMI.

Contenido

Configuración predeterminada

La configuración bloquear el acceso público a las AMI está habilitada o deshabilitada de forma predeterminada en función de si su cuenta es nueva o existente y de si tiene AMI públicas. En la tabla siguiente se muestra la configuración predeterminada:

Cuenta de AWS	Configuración bloquear el acceso público a las AMI
Cuentas nuevas	Habilitado
Cuentas existentes sin AMI públicas [1]	Habilitado
Cuentas existentes con una o varias AMI públicas	Deshabilitad

[1] Si su cuenta tenía una o varias AMI públicas el 15 de julio de 2023 o después de esa fecha, la configuración bloquear el acceso público a las AMI está deshabilitada de forma predeterminada en su cuenta, aunque posteriormente haya hecho que todas las AMI sean privadas.

Permisos de IAM necesarios

Para utilizar el bloqueo del acceso público de las AMI, debe contar con los siguientes permisos de IAM:

- `EnableImageBlockPublicAccess`
- `DisableImageBlockPublicAccess`
- `GetImageBlockPublicAccessState`

Habilitar el bloqueo del acceso público de las AMI

Para impedir que sus AMI se compartan públicamente, habilite el bloqueo del acceso público de las AMI a nivel de cuenta. Debe habilitar el bloqueo del acceso público de las AMI en cada Región de AWS en la que desea impedir que se compartan públicamente sus AMI. Si ya tiene AMI públicas, permanecerán disponibles públicamente.

Console

Para habilitar el bloqueo del acceso público de las AMI en la región especificada

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la barra de navegación (en la parte superior de la pantalla), seleccione la región en la que desea habilitar el bloqueo del acceso público de las AMI.
3. Si no se muestra el panel, en el panel de navegación, elija Panel de EC2.
4. En Atributos de la cuenta, elija Protección y seguridad de datos.
5. En bloqueo del acceso público de las AMI, elija Administrar.
6. Seleccione la casilla de verificación bloquear nuevo uso compartido público y luego, elija Actualizar.

> **Note**
>
> La API puede tardar hasta 10 minutos en configurar este ajuste. Durante este tiempo, el valor será Nuevo uso compartido público permitido. Cuando la API haya

completado la configuración, el valor cambiará de manera automática a Nuevo uso compartido público bloqueado.

AWS CLI

Para habilitar el bloqueo del acceso público de las AMI en la región especificada

Utilice el comando enable-image-block-public-access y especifique la región en la que se habilitará el bloqueo del acceso público de las AMI. En el parámetro `--image-block-public-access-state`, especifique `block-new-sharing`.

```
aws ec2 enable-image-block-public-access \
    --region us-east-1 \
    --image-block-public-access-state block-new-sharing
```

Resultado previsto

```
{
    "ImageBlockPublicAccessState": "block-new-sharing"
}
```

> **Note**
>
> La API puede tardar hasta 10 minutos en configurar este ajuste. Durante este tiempo, si ejecuta el comando get-image-block-public-access-state, la respuesta será `unblocked`. Cuando la API haya completado la configuración, la respuesta será `block-new-sharing`.

Deshabilitar el bloqueo del acceso público de las AMI

Para permitir que los usuarios de su cuenta compartan públicamente sus AMI, deshabilite el bloqueo del acceso público a nivel de cuenta. Debe deshabilitar el bloqueo del acceso público de las AMI en cada Región de AWS en la que desea permitir que se compartan públicamente sus AMI.

Console

Para deshabilitar el bloqueo del acceso público de las AMI en la región especificada

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la barra de navegación (en la parte superior de la pantalla), seleccione la región en la que desea deshabilitar el bloqueo del acceso público de las AMI.
3. Si no se muestra el panel, en el panel de navegación, elija Panel de EC2.
4. En Atributos de la cuenta, elija Protección y seguridad de datos.
5. En bloqueo del acceso público de las AMI, elija Administrar.
6. Desactive la casilla de verificación bloquear nuevo uso compartido público y luego, elija Actualizar.
7. Cuando se le pida confirmación, ingrese **`confirm`** y elija Permitir uso compartido.

> **Note**
>
> La API puede tardar hasta 10 minutos en configurar este ajuste. Durante este tiempo, el valor será Nuevo uso compartido público bloqueado. Cuando la API haya completado la configuración, el valor cambiará de manera automática a Nuevo uso compartido público permitido.

AWS CLI

Para deshabilitar el bloqueo del acceso público de las AMI en la región especificada

Utilice el comando disable-image-block-public-access y especifique la región en la que se deshabilitará el bloqueo del acceso público de las AMI.

```
aws ec2 disable-image-block-public-access --region us-east-1
```

Resultado previsto

```
{
   "ImageBlockPublicAccessState": "unblocked"
}
```

> **Note**
>
> La API puede tardar hasta 10 minutos en configurar este ajuste. Durante este tiempo, si ejecuta el comando get-image-block-public-access-state, la respuesta será `block-new-sharing`. Cuando la API haya completado la configuración, la respuesta será `unblocked`.

Ver el estado del bloqueo del acceso público de las AMI

Para comprobar si el uso compartido público de las AMI está bloqueado en su cuenta, puede ver el estado del bloqueo del acceso público de las AMI. Debe ver el estado en cada Región de AWS en la que desee comprobar si el uso compartido público de sus AMI está bloqueado.

Console

Para ver el estado del bloqueo del acceso público de las AMI en la región especificada

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la barra de navegación (en la parte superior de la pantalla), seleccione la región en la que desea ver el estado del bloqueo del acceso público de las AMI.
3. Si no se muestra el panel, en el panel de navegación, elija Panel de EC2.
4. En Atributos de la cuenta, elija Protección y seguridad de datos.
5. En bloqueo del acceso público de las AMI, active el campo Acceso público. El valor será Nuevo uso compartido público bloqueado o Nuevo uso compartido público permitido.

AWS CLI

Para obtener el estado del bloqueo del acceso público de las AMI en la región especificada

Utilice el comando get-image-block-public-access-state y especifique la región en la que desea obtener el bloqueo del acceso público de las AMI.

```
aws ec2 get-image-block-public-access-state --region us-east-1
```

Resultado previsto: el valor será `block-new-sharing` o `unblocked`.

```
{
```

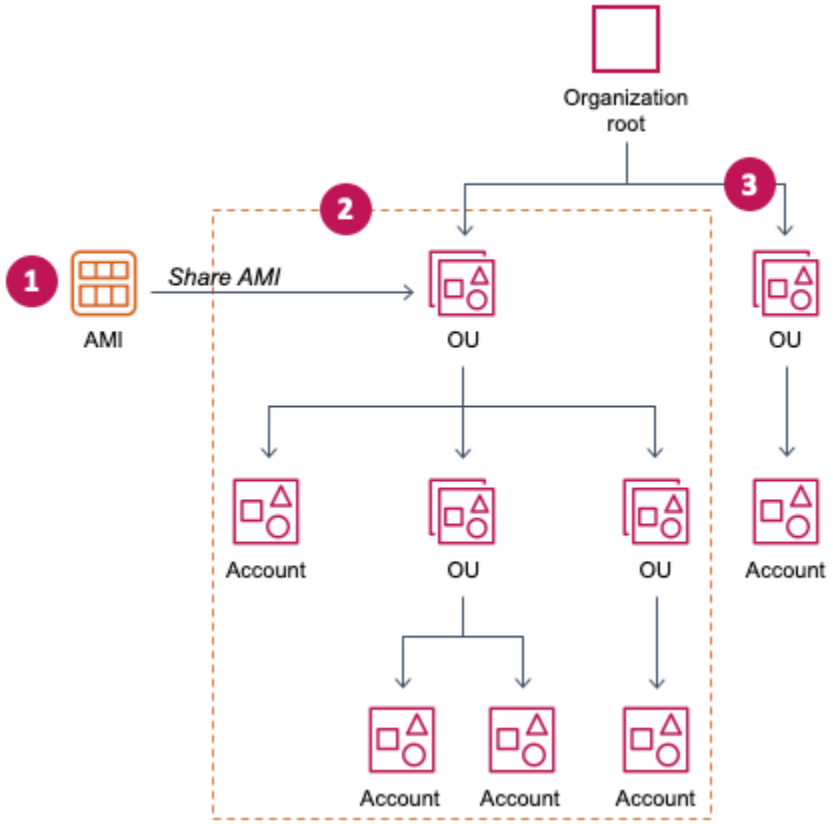
```
    "ImageBlockPublicAccessState": "block-new-sharing"
}
```

Compartir una AMI con organizaciones o unidades organizativas específicas

AWS Organizations es un servicio de administración de cuentas que le permite unificar varias Cuentas de AWS en una organización que crea y administra de forma centralizada. Puede compartir una AMI con una organización o una unidad organizativa (UO) de su creación, además de compartirla con cuentas específicas.

Una organización es una entidad que se crea para consolidar y administrar las Cuentas de AWS de forma centralizada. Puede organizar las cuentas jerárquicamente en una estructura de árbol con un nodo raíz en la parte superior y unidades organizativas anidadas bajo la organización raíz. Cada cuenta puede añadirse directamente en el nodo raíz o colocarse en una de las UO de la jerarquía. Para obtener más información, consulte Terminología y conceptos de AWS Organizations en la Guía del usuario de AWS Organizations.

Cuando comparte una AMI con una organización o una unidad organizativa, todas las cuentas secundarias obtienen acceso a la AMI. Por ejemplo, en el siguiente diagrama, la AMI se comparte con una unidad organizativa de nivel superior (indicada por la flecha en el número 1). Todas las unidades organizativas y cuentas anidadas debajo de esa unidad organizativa de nivel superior (indicadas por la línea punteada en el número 2) también tienen acceso a la AMI. Las cuentas de la organización y la unidad organizativa fuera de la línea punteada (indicadas por el número 3) no tienen acceso a la AMI porque no dependen de la unidad organizativa con la que se comparte la AMI.



Consideraciones

Tenga en cuenta lo siguiente al compartir AMI con organizaciones o unidades organizativas específicas.

- Propiedad: para compartir una AMI, su Cuenta de AWS debe ser la propietaria de esta.
- Límites del uso compartido: el propietario de la AMI puede compartir una AMI con cualquier organización o unidad organizativa, incluidas organizaciones y unidades organizativas de las que no son miembros.

  Para conocer el número máximo de entidades con las que se puede compartir una AMI dentro de una región, consulte Amazon EC2 service quotas.
- Etiquetas: no puede compartir etiquetas definidas por el usuario (etiquetas que se adjuntan a una AMI). Al compartir una AMI, las etiquetas definidas por el usuario no están disponibles para ninguna Cuenta de AWS de organización o unidad organizativa con la que se comparte la AMI.
- Formato ARN: al especificar una organización o UO en un comando, asegúrese de utilizar el formato ARN correcto. Si especifica solo el ID se producirá un error, por ejemplo, si solo especifica `o-123example` o `ou-1234-5example`.

Formatos de ARN adecuados:

- ARN de la organización: `arn:aws:organizations::account-id:organization/organization-id`
- ARN de la unidad organizativa: `arn:aws:organizations::account-id:ou/organization-id/ou-id`

Donde:

- *`account-id`* es el número de cuenta de administración de 12 dígitos, por ejemplo, `123456789012`. Si no conoce el número de cuenta de administración, puede describir la organización o la unidad organizativa para obtener el ARN, que incluye el número de cuenta de administración. Para obtener más información, consulte Obtener el ARN.
- *`organization-id`* es el ID de la organización, por ejemplo, `o-123example`.
- *`ou-id`* es el ID de la unidad organizativa, por ejemplo, `ou-1234-5example`.

Para obtener más información acerca del formato de los ARN, consulte Nombres de recursos de Amazon (ARN) en la Guía del usuario de IAM.

- Cifrado y claves: puede compartir AMI que cuentan con el respaldo de instantáneas sin cifrar y cifradas.
  - Las instantáneas cifradas deben estar cifradas con una clave administrada por el cliente. No pueden compartir las AMI que están respaldadas por instantáneas cifradas con la clave predeterminada administrada por AWS.
  - Si comparte una AMI basada en instantáneas cifradas, debe permitir que las organizaciones o unidades organizativas utilicen las claves administradas por el cliente que se utilizaron para cifrar las instantáneas. Para obtener más información, consulte Permitir que las organizaciones y unidades organizativas utilicen una clave de KMS.
- Región: las AMI son un recurso regional. Cuando comparte una AMI, solo está disponible en la región desde donde la compartió. Para hacer que una AMI esté disponible en una región distinta, copie la AMI en dicha región y, a continuación, compártala. Para obtener más información, consulte Copiar una AMI.
- Uso: cuando comparte una AMI, los usuarios solo pueden iniciar instancias desde la AMI. No pueden eliminarla, compartirla ni modificarla. Sin embargo, después de iniciar una instancia mediante la AMI, pueden crear una AMI a partir de esa instancia.
- Facturación: no se factura cuando otras Cuentas de AWS utilizan la AMI para iniciar instancias. Las cuentas que inician instancias mediante la AMI serán facturadas por las instancias iniciadas.

Permitir que las organizaciones y unidades organizativas utilicen una clave de KMS

Si comparte una AMI respaldada por instantáneas cifradas, también debe permitir que las organizaciones o unidades organizativas utilicen las AWS KMS keys que se utilizaron para cifrar las instantáneas.

Utilice las claves `aws:PrincipalOrgID` y `aws:PrincipalOrgPaths` para comparar la ruta de AWS Organizations de la entidad principal que realiza la solicitud a la ruta en la política. Una entidad principal puede ser un usuario, rol de IAM, usuario federado o usuario raíz de Cuenta de AWS. En una política, esta clave de condición garantiza que el solicitante es un miembro de la cuenta dentro de la raíz de la organización o unidad organizativa especificadas en AWS Organizations. Para ver más ejemplos de declaraciones de condiciones, consulte aws:PrincipalOrgID y aws:PrincipalOrgPaths en la Guía del usuario de IAM.

Para obtener más información sobre la modificación de una política de claves, consulte, Allowing users in other accounts to use a KMS key en la Guía para desarrolladores de AWS Key Management Service.

Para conceder permiso a una organización o unidad organizativa para utilizar una clave de KMS, agregue la siguiente instrucción a la política de claves.

```
{
    "Sid": "Allow access for organization root",
    "Effect": "Allow",
    "Principal": "*",
    "Action": [
        "kms:Describe*",
        "kms:List*",
        "kms:Get*",
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:PrincipalOrgID": "o-123example"
        }
    }
}
```

Para compartir una clave de KMS con varias unidades organizativas, puede utilizar una política similar a la del siguiente ejemplo.

```
{
        "Sid": "Allow access for specific OUs and their descendants",
        "Effect": "Allow",
        "Principal": "*",
        "Action": [
            "kms:Describe*",
            "kms:List*",
            "kms:Get*",
            "kms:Encrypt",
            "kms:Decrypt",
            "kms:ReEncrypt*",
            "kms:GenerateDataKey*"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:PrincipalOrgID": "o-123example"
            },
            "ForAnyValue:StringLike": {
                "aws:PrincipalOrgPaths": [
                    "o-123example/r-ab12/ou-ab12-33333333/*",
                    "o-123example/r-ab12/ou-ab12-22222222/*"
                ]
            }
        }
}
```

Compartir una AMI

Puede utilizar la consola de Amazon EC2 o la AWS CLI para compartir una AMI con una organización o una unidad organizativa.

Compartir una AMI (consola)

Para compartir una AMI con una organización o una unidad organizativa mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione AMIs.
3. Seleccione la AMI en la lista y, a continuación, elija Acciones, Editar permisos de la AMI.

4. En Disponibilidad de AMI, elija Privada.
5. Junto a Organizaciones/unidades organizativas compartidas, elija Agregar ARN de organización/unidad organizativa.
6. En ARN de organización/unidad organizativa, introduzca el ARN de la organización o de la unidad organizativa con el que desea compartir la AMI y, a continuación, elija Compartir AMI. Tenga en cuenta que debe especificar el ARN completo, no solo el ID.

   Para compartir esta AMI con varias organizaciones o unidades organizativas, repita este paso hasta que haya agregado todas las organizaciones o unidades organizativas necesarias.

   > **Note**
   >
   > No es necesario compartir las instantáneas de Amazon EBS a las que hace referencia una AMI para compartir dicha AMI. Solo es necesario compartir la AMI; para la inicialización, el sistema proporciona automáticamente a la instancia acceso a las instantáneas de Amazon EBS a las que se hace referencia. Sin embargo, es necesario compartir las claves de KMS que se utilizan para cifrar instantáneas a las que hace referencia la AMI. Para obtener más información, consulte Permitir que las organizaciones y unidades organizativas utilicen una clave de KMS.

7. Cuando haya terminado, elija Guardar cambios.
8. (Opcional) Para ver las organizaciones o unidades organizativas con las que ha compartido la AMI, seleccione la AMI en la lista, elija la pestaña Permisos y desplácese hacia abajo hasta Organizaciones/unidades organizativas compartidas. Para encontrar las AMI compartidas con usted, consulte Buscar AMI compartidas.

Compartir una AMI (Herramientas para Windows PowerShell)

Utilice el comando Edit-EC2ImageAttribute (Herramientas para Windows PowerShell) para compartir una AMI tal y como se muestra en los siguientes ejemplos.

Para compartir una AMI con una organización o una unidad organizativa

El siguiente comando concede permisos de inicialización para la AMI especificada a la organización determinada.

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -
Attribute launchPermission -OperationType add -OrganizationArn
 "arn:aws:organizations::123456789012:organization/o-123example"
```

> **Note**
>
> No es necesario compartir las instantáneas de Amazon EBS a las que hace referencia una AMI para compartir dicha AMI. Solo es necesario compartir la AMI; para la inicialización, el sistema proporciona automáticamente a la instancia acceso a las instantáneas de Amazon EBS a las que se hace referencia. Sin embargo, es necesario compartir las claves de KMS que se utilizan para cifrar instantáneas a las que hace referencia la AMI. Para obtener más información, consulte Permitir que las organizaciones y unidades organizativas utilicen una clave de KMS.

Para dejar de compartir una AMI con una organización o unidad organizativa

El siguiente comando elimina permisos de inicialización para la AMI especificada de la organización determinada:

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -
Attribute launchPermission -OperationType remove -OrganizationArn
 "arn:aws:organizations::123456789012:organization/o-123example"
```

Para dejar de compartir una AMI con todas las organizaciones, unidades organizativas y Cuentas de AWS

El siguiente comando elimina todos los permisos de inicialización públicos y explícitos de la AMI especificada. Tenga en cuenta que el propietario de la AMI siempre tiene permisos de inicialización, por lo que este comando no le afecta.

```
PS C:\> Reset-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute
 launchPermission
```

Compartir una AMI (AWS CLI)

Utilice el comando modify-image-attribute (AWS CLI) para compartir una AMI.

Para compartir una AMI con una organización mediante la AWS CLI

El comando modify-image-attribute concede permisos de inicialización para la AMI especificada a la organización determinada. Tenga en cuenta que debe especificar el ARN completo, no solo el ID.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission
 "Add=[{OrganizationArn=arn:aws:organizations::123456789012:organization/
o-123example}]"
```

Para compartir una AMI con una unidad organizativa mediante la AWS CLI

El comando modify-image-attribute concede permisos de inicialización para la AMI especificada a la unidad organizativa determinada. Tenga en cuenta que debe especificar el ARN completo, no solo el ID.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission
 "Add=[{OrganizationalUnitArn=arn:aws:organizations::123456789012:ou/o-123example/
ou-1234-5example}]"
```

> **Note**
>
> No es necesario compartir las instantáneas de Amazon EBS a las que hace referencia una AMI para compartir dicha AMI. Solo es necesario compartir la AMI; para la inicialización, el sistema proporciona automáticamente a la instancia acceso a las instantáneas de Amazon EBS a las que se hace referencia. Sin embargo, es necesario compartir las claves de KMS que se utilizan para cifrar instantáneas a las que hace referencia la AMI. Para obtener más información, consulte Permitir que las organizaciones y unidades organizativas utilicen una clave de KMS.

Dejar de compartir una AMI

Puede utilizar la consola de Amazon EC2 o la AWS CLI para dejar de compartir una AMI con una organización o una unidad organizativa.

Dejar de compartir una AMI (consola)

Para dejar de compartir una AMI con una organización o una unidad organizativa mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione AMIs.
3. Seleccione la AMI en la lista y, a continuación, elija Actions (Acciones), Edit AMI permissions (Editar permisos de la AMI).
4. En Organizaciones/unidades organizativas compartidas, seleccione las organizaciones o unidades organizativas con las que desea dejar de compartir la AMI y, a continuación, elija Eliminar la selección.
5. Cuando haya terminado, elija Guardar cambios.
6. (Opcional) Para confirmar que dejó de compartir la AMI con las organizaciones o unidades organizativas, seleccione la AMI en la lista, elija la pestaña Permisos y desplácese hacia abajo hasta Organizaciones/unidades organizativas compartidas.

Dejar de compartir una AMI (AWS CLI)

Utilice los comandos modify-image-attribute o reset-image-attribute (AWS CLI) para dejar de compartir una AMI.

Para dejar de compartir una AMI con una organización o una unidad organizativa mediante la AWS CLI

El comando modify-image-attribute elimina permisos de inicialización para la AMI especificada de la organización determinada. Tenga en cuenta que debe especificar el ARN.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission
 "Remove=[{OrganizationArn=arn:aws:organizations::123456789012:organization/
o-123example}]"
```

Para dejar de compartir una AMI con todas las organizaciones, unidades organizativas y Cuentas de AWS mediante la AWS CLI

El comando reset-image-attribute elimina todos los permisos de inicialización públicos y explícitos de la AMI especificada. Tenga en cuenta que el propietario de la AMI siempre tiene permisos de inicialización, por lo que este comando no le afecta.

```
aws ec2 reset-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --attribute launchPermission
```

> **Note**
>
> No puede dejar de compartir una AMI con una cuenta específica si se encuentra en una organización o unidad organizativa con la que se comparte una AMI. Si intenta dejar de compartir la AMI mediante la eliminación de los permisos de inicialización de la cuenta, Amazon EC2 devuelve el mensaje de que la operación se realizó correctamente. Sin embargo, la AMI sigue compartiéndose con la cuenta.

Ver las organizaciones y unidades organizativas con las que se comparte una AMI

Para verificar con qué organizaciones y unidades organizativas compartió la AMI, puede utilizar la consola de Amazon EC2 o la AWS CLI.

Ver las organizaciones y unidades organizativas con las que se comparte una AMI (consola)

Para verificar con qué organizaciones y unidades organizativas compartió la AMI mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione AMIs.
3. Seleccione la AMI en la lista, elija la pestaña Permisos y desplácese hacia abajo hasta Organizaciones/unidades organizativas compartidas.

   Para encontrar las AMI compartidas con usted, consulte Buscar AMI compartidas.

Ver las organizaciones y unidades organizativas con las que se comparte una AMI (AWS CLI)

Puede verificar con qué organizaciones y unidades organizativas compartió la AMI mediante el comando describe-image-attribute (AWS CLI) y el atributo `launchPermission`.

Para verificar con qué organizaciones y unidades organizativas compartió la AMI mediante la AWS CLI

El comando describe-image-attribute describe el atributo `launchPermission` de la AMI especificada y muestra las organizaciones y unidades organizativas con las que la compartió.

```
aws ec2 describe-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --attribute launchPermission
```

Ejemplo de respuesta

```
{
    "ImageId": "ami-0abcdef1234567890",
    "LaunchPermissions": [
        {
            "OrganizationalUnitArn": "arn:aws:organizations::111122223333:ou/
o-123example/ou-1234-5example"
        }
    ]
}
```

Obtener el ARN

La organización y los ARN de la unidad organizativa contienen el número de cuenta de administración de 12 dígitos. Si no conoce el número de cuenta de administración, puede describir la organización y la unidad organizativa para obtener el ARN de cada una. En los siguientes ejemplos, `123456789012` es el número de cuenta de administración.

Para poder obtener los ARN, debe tener permiso para describir organizaciones y unidades organizativas. La siguiente política de ejemplo proporciona el permiso necesario.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:Describe*"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

Para obtener el ARN de una organización

Utilice el comando describe-organization y el parámetro `--query` establecido en `'Organization.Arn'` para devolver solo el ARN de la organización.

```
aws organizations describe-organization --query 'Organization.Arn'
```

Ejemplo de respuesta

```
"arn:aws:organizations::123456789012:organization/o-123example"
```

Para obtener el ARN de una unidad organizativa

Utilice el comando describe-organizational-unit, especifique el ID de la unidad organizativa y establezca el parámetro `--query` en `'OrganizationalUnit.Arn'` para devolver solo el ARN de la unidad organizativa.

```
aws organizations describe-organizational-unit --organizational-unit-
id ou-1234-5example --query 'OrganizationalUnit.Arn'
```

Ejemplo de respuesta

```
"arn:aws:organizations::123456789012:ou/o-123example/ou-1234-5example"
```

Compartir una AMI con cuentas de AWS específicas

Puede compartir una AMI con Cuentas de AWS específicas sin hacerla pública. Lo único que necesita es las ID de Cuenta de AWS.

Un identificador de Cuenta de AWS es un número de 12 dígitos, por ejemplo `012345678901`, que identifica de forma única a una Cuenta de AWS. Para obtener más información, consulte Visualización de identificadores de la Cuenta de AWS en la Guía de referencia de AWS Account Management.

Consideraciones

Tenga en cuenta lo siguiente al compartir AMI con Cuentas de AWS específicas.

- Propiedad: para compartir una AMI, su Cuenta de AWS debe ser la propietaria de esta.
- Límites del uso compartido: para conocer el número máximo de entidades con las que se puede compartir una AMI dentro de una región, consulte Amazon EC2 service quotas.
- Etiquetas: no puede compartir etiquetas definidas por el usuario (etiquetas que se adjuntan a una AMI). Al compartir una AMI, las etiquetas definidas por el usuario no están disponibles para ninguna de las personas de las Cuenta de AWS que comparten la AMI.
- Cifrado y claves: puede compartir AMI que cuentan con el respaldo de instantáneas sin cifrar y cifradas.
  - Las instantáneas cifradas deben estar cifradas con una clave de KMS. No pueden compartir las AMI que están respaldadas por instantáneas cifradas con la clave predeterminada administrada por AWS.
  - Si comparte una AMI respaldada por instantáneas cifradas, debe permitir que las Cuentas de AWS utilicen las claves administradas por el cliente que se utilizaron para cifrar las instantáneas. Para obtener más información, consulte Permitir que las organizaciones y unidades organizativas utilicen una clave de KMS. Para configurar la política de claves que necesita para iniciar instancias de Auto Scaling cuando utiliza una clave administrada por el cliente para el cifrado, consulte Política requerida AWS KMS key para usar con volúmenes cifrados en la Guía del usuario de Amazon EC2 Auto Scaling.
- Región: las AMI son un recurso regional. Cuando comparte una AMI, solo estará disponible en esa región. Para hacer que una AMI esté disponible en una región distinta, copie la AMI en dicha región y, a continuación, compártala. Para obtener más información, consulte Copiar una AMI.
- Uso: cuando comparte una AMI, los usuarios solo pueden iniciar instancias desde la AMI. No pueden eliminarla, compartirla ni modificarla. Sin embargo, después de iniciar una instancia mediante la AMI, pueden crear una AMI a partir de esa instancia.
- Copiar AMI compartidas: si los usuarios de otra cuenta desean copiar una AMI compartida, debe otorgar permisos de lectura para el almacenamiento que respalda la AMI. Para obtener más información, consulte Copias entre cuentas.
- Facturación: no se factura cuando otras Cuentas de AWS utilizan la AMI para iniciar instancias. Las cuentas que inician instancias mediante la AMI serán facturadas por las instancias iniciadas.

Compartir una AMI (consola)

Para conceder permisos de inicialización explícito mediante la consola

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

2. En el panel de navegación, seleccione AMIs.
3. Seleccione la AMI en la lista y, a continuación, elija Actions (Acciones), Edit AMI permissions (Editar permisos de la AMI).
4. Seleccione Privado.
5. En Cuentas compartidas, elija Agregar ID de cuenta.
6. En ID de la Cuenta de AWS, ingrese el ID de la Cuenta de AWS con la que desea compartir la AMI y, a continuación, elija Compartir AMI.

   Para compartir esta AMI con varias cuentas, repita los pasos 5 y 6 hasta que haya agregado todos los ID de cuenta necesarios.

   > **Note**
   >
   > No es necesario compartir las instantáneas de Amazon EBS a las que hace referencia una AMI para compartir dicha AMI. Solo es necesario compartir la propia AMI; el sistema proporciona automáticamente a la instancia acceso a las instantáneas de Amazon EBS a las que se hace referencia para la inicialización. Sin embargo, es necesario compartir las Claves de KMS que se utilizan para cifrar instantáneas a las que hace referencia la AMI. Para obtener más información, consulte Compartir una instantánea de Amazon EBS en la Guía del usuario de Amazon EBS.

7. Cuando haya terminado, elija Guardar cambios.
8. (Opcional) Para ver los ID de la Cuenta de AWS con los que ha compartido la AMI, seleccione la AMI en la lista y elija la pestaña Permisos. Para encontrar las AMI compartidas con usted, consulte Buscar AMI compartidas.

Compartir una AMI (Herramientas para Windows PowerShell)

Utilice el comando Edit-EC2ImageAttribute (Herramientas para Windows PowerShell) para compartir una AMI tal y como se muestra en los siguientes ejemplos.

Para conceder permisos de inicialización explícitos

El siguiente comando concede permisos de inicialización para la AMI especificada a la Cuenta de AWS especificada. En el siguiente ejemplo, reemplace el ID de AMI de ejemplo con un ID de AMI válido y reemplace *account-id* con el ID de Cuenta de AWS de 12 dígitos.

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute
 launchPermission -OperationType add -UserId "account-id"
```

> **Note**
>
> No es necesario compartir las instantáneas de Amazon EBS a las que hace referencia una AMI para compartir dicha AMI. Solo es necesario compartir la propia AMI; el sistema proporciona automáticamente a la instancia acceso a las instantáneas de Amazon EBS a las que se hace referencia para la inicialización. Sin embargo, es necesario compartir las Claves de KMS que se utilizan para cifrar instantáneas a las que hace referencia la AMI. Para obtener más información, consulte Compartir una instantánea de Amazon EBS en la Guía del usuario de Amazon EBS.

Para eliminar permisos de inicialización para una cuenta

El siguiente comando elimina permisos de inicialización para la AMI especificada de la Cuenta de AWS especificada. En el siguiente ejemplo, reemplace el ID de AMI de ejemplo con un ID de AMI válido y reemplace *account-id* con el ID de Cuenta de AWS de 12 dígitos.

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute
 launchPermission -OperationType remove -UserId "account-id"
```

Para eliminar todos los permisos de inicialización

El siguiente comando elimina todos los permisos de inicialización públicos y explícitos de la AMI especificada. Tenga en cuenta que el propietario de la AMI siempre tiene permisos de inicialización, por lo que este comando no le afecta. En el siguiente ejemplo, reemplace el ID de AMI de ejemplo con un ID de AMI válido.

```
PS C:\> Reset-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute
 launchPermission
```

Compartir una AMI (AWS CLI)

Utilice el comando modify-image-attribute (AWS CLI) para compartir una AMI tal y como se muestra en los siguientes ejemplos.

Para conceder permisos de inicialización explícitos

El siguiente comando concede permisos de inicialización para la AMI especificada a la Cuenta de AWS especificada. En el siguiente ejemplo, reemplace el ID de AMI de ejemplo con un ID de AMI válido y reemplace *account-id* con el ID de Cuenta de AWS de 12 dígitos.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission "Add=[{UserId=account-id}]"
```

> **Note**
>
> No es necesario compartir las instantáneas de Amazon EBS a las que hace referencia una AMI para compartir dicha AMI. Solo es necesario compartir la propia AMI; el sistema proporciona automáticamente a la instancia acceso a las instantáneas de Amazon EBS a las que se hace referencia para la inicialización. Sin embargo, es necesario compartir las Claves de KMS que se utilizan para cifrar instantáneas a las que hace referencia la AMI. Para obtener más información, consulte Compartir una instantánea de Amazon EBS en la Guía del usuario de Amazon EBS.

Para eliminar permisos de inicialización para una cuenta

El siguiente comando elimina permisos de inicialización para la AMI especificada de la Cuenta de AWS especificada. En el siguiente ejemplo, reemplace el ID de AMI de ejemplo con un ID de AMI válido y reemplace *account-id* con el ID de Cuenta de AWS de 12 dígitos.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission "Remove=[{UserId=account-id}]"
```

Para eliminar todos los permisos de inicialización

El siguiente comando elimina todos los permisos de inicialización públicos y explícitos de la AMI especificada. Tenga en cuenta que el propietario de la AMI siempre tiene permisos de inicialización, por lo que este comando no le afecta. En el siguiente ejemplo, reemplace el ID de AMI de ejemplo con un ID de AMI válido.

```
aws ec2 reset-image-attribute \
```

```
    --image-id ami-0abcdef1234567890 \
    --attribute launchPermission
```

Cancelar que se comparta una AMI con su Cuenta de AWS

Se puede compartir una imagen de máquina de Amazon (AMI) con Cuentas de AWS específicas si agrega las cuentas a los permisos de inicialización de la AMI. Si se ha compartido una AMI con su Cuenta de AWS y ya no desea que sea así, puede eliminar la cuenta de los permisos de inicialización de la AMI. Para hacerlo, ejecute el comando `cancel-image-launch-permission` de la AWS CLI. Al ejecutar este comando, la Cuenta de AWS se elimina de los permisos de inicialización de la AMI especificada.

Puede cancelar que se comparta una AMI con la cuenta, por ejemplo, para reducir la probabilidad de iniciar una instancia con una AMI obsoleta o en desuso que se compartió con usted. Cuando cancele que se comparta una AMI con la cuenta, ya no aparecerá en ninguna lista de AMI de la consola de EC2 ni en la salida de describe-images.

Temas

Limitaciones

- Puede eliminar la cuenta de los permisos de inicialización de una AMI compartida solo con su Cuenta de AWS. No puede usar `cancel-image-launch-permission` para eliminar la cuenta de los permisos de inicialización de una AMI compartida con una organización o unidad organizativa ni para eliminar el acceso a las AMI públicas.
- No puede eliminar permanentemente su cuenta de los permisos de inicialización de una AMI. El propietario de una AMI puede volver a compartirla con su cuenta.
- Las AMI son un recurso regional. Al ejecutar `cancel-image-launch-permission`, debe especificar la región en la que se encuentra la AMI. Para especificar una región predeterminada en el comando, utilice la variable de entorno AWS_DEFAULT_REGION.
- Solo la AWS CLI y los SDK admiten que se elimine la cuenta de los permisos de inicialización de una AMI. Actualmente, la consola de EC2 no admite esta acción.

Cancelar que se comparta una AMI con su cuenta

> **Note**
>
> Después de cancelar que se comparta una AMI con la cuenta, no podrá deshacer la acción. Para recuperar el acceso a la AMI, el propietario de esta debe compartirla con su cuenta.

AWS CLI

Para cancelar que se comparta una AMI con su Cuenta de AWS

Utilice el comando cancel-image-launch-permission y especifique el ID de la AMI.

```
aws ec2 cancel-image-launch-permission \
    --image-id ami-0123456789example \
    --region us-east-1
```

Resultado previsto

```
{
    "Return": true
}
```

PowerShell

Para cancelar que se comparta una AMI con su Cuenta de AWS mediante AWS Tools for PowerShell

Utilice el comando Stop-EC2ImageLaunchPermission y especifique el ID de la AMI.

```
Stop-EC2ImageLaunchPermission `
    -ImageId ami-0123456789example `
    -Region us-east-1
```

Resultado previsto

```
True
```

Encuentre las AMI compartidas con su cuenta

Para encontrar las AMI compartidas con su Cuenta de AWS, consulte Buscar AMI compartidas.

Usar marcadores

Si ha creado una AMI pública o ha compartido una AMI con otra Cuenta de AWS, puede crear un marcador que permita al usuario obtener acceso a la AMI y iniciar una instancia en su propia cuenta inmediatamente. Esta es una forma sencilla de compartir referencias de AMI para que los usuarios no tengan que dedicar tiempo a encontrar la AMI para poder usarla.

Tenga en cuenta que la AMI debe ser pública o debe haberla compartido con el usuario a quien desea enviar el marcador.

Para crear un marcador para la AMI

1. Escriba una dirección URL con la siguiente información, en la que region es la región en la que reside la AMI:

   ```
   https://console.aws.amazon.com/ec2/v2/home?
   region=region#LaunchInstanceWizard:ami=ami_id
   ```

   Por ejemplo, esta URL inicia una instancia desde la AMI ami-0abcdef1234567890 en la región `us-east-1` del Este de EE. UU. (Norte de Virginia):

   ```
   https://console.aws.amazon.com/ec2/v2/home?region=us-
   east-1#LaunchInstanceWizard:ami=ami-0abcdef1234567890
   ```

2. Distribuya el enlace a los usuarios que desean usar la AMI.
3. Para usar un marcador, elija el enlace o cópielo y péguelo en el navegador. Se abrirá el launch wizard con la AMI ya seleccionada.

Directrices para AMI de Linux compartidas

Utilice las siguientes directrices para reducir la superficie de ataque y mejorar la fiabilidad de las AMI que cree.

> **Important**
>
> Ninguna lista de directrices de seguridad es exhaustiva. Cree sus AMI compartidas con precaución y piense bien en qué casos podría estar exponiendo información confidencial.

Contenido

Si crea la AMI para AWS Marketplace, consulte Prácticas recomendadas para crear AMI en la Guía del vendedor de AWS Marketplace en lo que respecta a directrices, políticas y prácticas recomendadas.

Para obtener información adicional sobre cómo compartir AMI de forma segura, consulte los siguientes artículos:

- Cómo compartir y utilizar AMI públicas de una forma segura
- Publicación de AMI públicas: requisitos de protección y limpieza

Actualizar las herramientas de AMI antes de usarlas

Para las AMI con el respaldado del almacén de instancias, le recomendamos que descargue y actualice las herramientas de creación de AMI de Amazon EC2 antes de utilizarlas. Esto garantiza que las nuevas AMI basadas en las AMI compartidas tengan las últimas herramientas para AMI.

En Amazon Linux 2, instale el paquete `aws-amitools-ec2` y añada las herramientas de la AMI a PATH con el comando siguiente. En Amazon Linux AMI, el paquete `aws-amitools-ec2` ya está instalado de forma predeterminada.

```
[ec2-user ~]$ sudo yum install -y aws-amitools-ec2 && export PATH=$PATH:/opt/aws/bin
 > /etc/profile.d/aws-amitools-ec2.sh && . /etc/profile.d/aws-amitools-ec2.sh
```

Actualice las herramientas de la AMI con el siguiente comando:

```
[ec2-user ~]$ sudo yum upgrade -y aws-amitools-ec2
```

Para otras distribuciones, asegúrese de tener las últimas herramientas para AMI.

Deshabilitación de los inicios de sesión remotos mediante contraseña para el usuario raíz

El uso de una contraseña raíz fija para una AMI pública supone un riesgo para la seguridad que puede darse a conocer rápidamente. Incluso pedir a los usuarios que cambien la contraseña tras el primer inicio de sesión abre la puerta a un potencial abuso.

Para solucionar este problema, deshabilite los inicios de sesión remotos mediante contraseña para el usuario raíz.

Deshabilitar los inicios de sesión remotos mediante contraseña para el usuario raíz

1. Abra el archivo `/etc/ssh/sshd_config` con un editor de texto y localice la siguiente línea:

   ```
   #PermitRootLogin yes
   ```

2. Cambie la línea a:

   ```
   PermitRootLogin without-password
   ```

   La ubicación de este archivo de configuración podría diferir para su distribución o si no está ejecutando OpenSSH. En ese caso, consulte la documentación pertinente.

Deshabilitar el acceso local de la raíz

Cuando trabaja con AMI compartidas, es una práctica recomendada deshabilitar los inicios de sesión directos de la raíz. Para ello, inicie sesión en la instancia en ejecución e introduzca el siguiente comando:

```
[ec2-user ~]$ sudo passwd -l root
```

> **Note**
>
> Este comando no afecta al uso de `sudo`.

Eliminar los pares de claves del host SSH

Si tiene previsto compartir una AMI derivada de una AMI pública, elimine los pares de claves del host de SSH existentes ubicados en `/etc/ssh`. Esto obliga a SSH a generar nuevos pares de claves de SSH únicos cuando alguien inicia una instancia usando la AMI, lo que mejora la seguridad y reduce la probabilidad de ataques "man-in-the-middle" (MITM).

Elimine los siguientes archivos de claves presentes en el sistema.

- ssh_host_dsa_key
- ssh_host_dsa_key.pub
- ssh_host_key
- ssh_host_key.pub
- ssh_host_rsa_key
- ssh_host_rsa_key.pub
- ssh_host_ecdsa_key
- ssh_host_ecdsa_key.pub
- ssh_host_ed25519_key
- ssh_host_ed25519_key.pub

Puede eliminar de forma segura todos esos archivos con el comando siguiente.

```
[ec2-user ~]$ sudo shred -u /etc/ssh/*_key /etc/ssh/*_key.pub
```

> **Warning**
>
> Los servicios de eliminación segura, como **`shred`**, podrían no eliminar todas las copias de un archivo del medio de almacenamiento. Los sistemas de archivos de registro en diario (incluidos Amazon Linux default ext4), las instantáneas, las copias de seguridad, los RAID y

el almacenamiento temporal en caché podrían crear copias ocultas de archivos. Para obtener más información, consulte la documentación de **`shred`**.

> **Important**
>
> Si olvida eliminar los pares de claves del host de SSH existentes de la AMI pública, nuestro proceso de auditoría rutinario le notifica a usted y a todos los clientes que ejecuten instancias de la AMI acerca del posible riesgo para la seguridad. Tras un breve periodo de gracia, marcamos la AMI como privada.

Instalar credenciales de clave pública

Tras configurar la AMI para evitar el inicio de sesión mediante contraseña, debe asegurarse de que los usuarios pueden iniciar sesión utilizando otro mecanismo.

Amazon EC2 permite a los usuarios especificar un nombre de par de claves pública y privada para iniciar la instancia. Cuando se proporciona un nombre de par de claves válido durante la llamada a la API `RunInstances` (o a través de las herramientas de la API de la línea de comandos), la clave pública (la parte del par de claves que Amazon EC2 conserva en el servidor tras llamar a `CreateKeyPair` o a `ImportKeyPair`) se pone a disposición de la instancia a través de una consulta HTTP a los metadatos de dicha instancia.

Para iniciar sesión mediante SSH, la AMI debe recuperar el valor de la clave al arrancar y adjuntarlo a `/root/.ssh/authorized_keys` (o el equivalente para cualquier otra cuenta de usuario de la AMI). Los usuarios pueden iniciar instancias de la AMI con un par de claves e iniciar sesión sin necesidad de una contraseña raíz.

Muchas distribuciones, como Amazon Linux y Ubuntu, usan el paquete `cloud-init` para introducir credenciales de clave pública para un usuario configurado. Si su distribución no admite `cloud-init`, puede añadir el siguiente código a un script de arranque del sistema (como `/etc/rc.local`) para obtener la clave pública que especificó durante la inicialización para el usuario raíz.

> **Note**
>
> En el ejemplo siguiente, la dirección IP http://169.254.169.254/ es una dirección local del vínculo y solo es válida desde la instancia.

IMDSv2

```
if [ ! -d /root/.ssh ] ; then
        mkdir -p /root/.ssh
        chmod 700 /root/.ssh
fi
# Fetch public key using HTTP
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-
token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/public-keys/0/openssh-key > /tmp/my-key
if [ $? -eq 0 ] ; then
        cat /tmp/my-key >> /root/.ssh/authorized_keys
        chmod 700 /root/.ssh/authorized_keys
        rm /tmp/my-key
fi
```

IMDSv1

```
if [ ! -d /root/.ssh ] ; then
        mkdir -p /root/.ssh
        chmod 700 /root/.ssh
fi
# Fetch public key using HTTP
curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key > /tmp/my-key
if [ $? -eq 0 ] ; then
        cat /tmp/my-key >> /root/.ssh/authorized_keys
        chmod 700 /root/.ssh/authorized_keys
        rm /tmp/my-key
fi
```

Esto se puede aplicar a cualquier usuario; no es necesario restringirlo al usuario `root`.

> **Note**
>
> La reagrupación de una instancia basada en esta AMI incluye la clave con la que se lanzó. Para evitar que se incluya esta clave, debe borrar (o eliminar) el archivo `authorized_keys` o excluirlo de la reagrupación.

Desactivación de la verificación de DNS de sshd (opcional)

Deshabilitar la verificación de DNS de sshd debilita ligeramente la seguridad sshd. No obstante, si la resolución de DNS falla, los inicios de sesión SSH siguen funcionando. Si no deshabilita la verificación de sshd, los errores de resolución de DNS impedirán cualquier inicio de sesión.

Para deshabilitar la verificación de DNS de sshd

1. Abra el archivo `/etc/ssh/sshd_config` con un editor de texto y localice la siguiente línea:

```
#UseDNS yes
```

2. Cambie la línea a:

```
UseDNS no
```

> **Note**
>
> La ubicación de este archivo de configuración puede diferir para su distribución o si no está ejecutando OpenSSH. En ese caso, consulte la documentación pertinente.

Protéjase

Desaconsejamos el almacenamiento de información confidencial o software en cualquier AMI que comparta. Los usuarios que lancen una AMI compartida podrían reagruparla y registrarla como propia. Siga estas directrices para ayudarle a evitar ciertos riesgos para la seguridad que suelen pasarse por alto.

- Le recomendamos que utilice la opción `--exclude` *`directory`* en `ec2-bundle-vol` para omitir cualquier directorio y subdirectorio que contenga información secreta que no desearía incluir en el paquete. En particular, excluya todos los pares de claves pública y privada SSH propiedad de los usuarios y los archivos SSH `authorized_keys` cuando realice la agrupación de la imagen. Las AMI públicas de Amazon los almacenan en `/root/.ssh` para el usuario raíz y en `/home/`*`user_name`*`/.ssh/` para usuarios normales. Para obtener más información, consulte ec2-bundle-vol.

- Elimine siempre el historial del shell antes de realizar la agrupación. Si intenta cargar más de una agrupación en la misma AMI, el historial del shell contiene la clave de acceso. El siguiente ejemplo debería ser el último comando que ejecute antes de realizar la agrupación desde la instancia.

```
[ec2-user ~]$ shred -u ~/.*history
```

> **Warning**
>
> Las limitaciones de **`shred`** descritas en la advertencia anterior también son aplicables aquí.
> Tenga en cuenta que bash escribe el historial de la sesión actual en el disco al salir. Si cierra sesión en la instancia después de eliminar `~/.bash_history` y, a continuación, vuelve a iniciar sesión, verá que `~/.bash_history` se ha vuelto a crear y que contiene todos los comandos que ejecutó durante la sesión anterior.
> Además de bash, otros programas también escriben el historial en el disco. Tenga precaución y elimine o excluya los dot-files y dot-directories que no sean necesarios.

- La agrupación de una instancia en ejecución requiere la clave privada y el certificado X.509. Guarde estas y otras credenciales en un lugar que no forme parte de la agrupación (como, por ejemplo, el almacén de instancias).

AMI de pago

Una AMI pagada es una AMI que está a la venta en AWS Marketplace. AWS Marketplace es un almacenamiento en línea donde puede comprar software que se ejecuta en AWS; incluidas las AMI que se utilizan para iniciar la instancia de EC2. Las AMI de AWS Marketplace se organizan en categorías, como herramientas para desarrolladores, con el fin de permitirle encontrar productos que se adapten a sus necesidades. Para más información acerca de AWS Marketplace, vea el sitio web de AWS Marketplace.

Puede adquirir AMI de un tercero en AWS Marketplace, como las AMI que se incluyen en los contratos de servicio de organizaciones como Red Hat. También puede crear una AMI y venderla a otros usuarios de Amazon EC2 en AWS Marketplace. La creación de una AMI segura y útil para el consumo público es un proceso bastante sencillo si se siguen unas directrices muy simples. Para obtener información acerca de cómo crear y utilizar AMI compartidas, consulte AMI compartidas.

iniciar una instancia desde una AMI de pago es lo mismo que iniciarla desde cualquier otra AMI. No se requieren más parámetros. La instancia se paga de acuerdo con las tarifas que establece el propietario de la AMI, así como las tarifas de uso estándar de los servicios web relacionados; por ejemplo, la tarifa por hora de ejecutar un tipo de instancia m5.small en Amazon EC2. Podrían aplicarse impuestos adicionales. El propietario de la AMI de pago puede confirmar si una instancia concreta se lanzó utilizando la AMI de pago.

> **Important**
>
> Amazon DevPay ya no acepta nuevos vendedores o productos. AWS Marketplace es ahora la única plataforma de comercio electrónico unificada para la venta de software y servicios a través de AWS. Para obtener información acerca de cómo implementar y vender software desde AWS Marketplace, consulte Selling in AWS Marketplace. AWS Marketplace admite las AMI respaldadas por Amazon EBS.

Contenido

Vender una AMI

Puede vender la AMI mediante AWS Marketplace. AWS Marketplace ofrece una experiencia de compra organizada. Además, AWS Marketplace también admite características de AWS como puede ser el caso de las AMI basadas en Amazon EBS, las instancias reservadas o las instancias de spot.

Para obtener información acerca de cómo vender la AMI en AWS Marketplace, consulte Selling in AWS Marketplace.

Buscar una AMI de pago

Hay varias formas de buscar AMI disponibles para comprarlas. Por ejemplo, puede utilizar AWS Marketplace, la consola de Amazon EC2 o la línea de comandos. Del mismo modo, un desarrollador puede informarle sobre alguna AMI de pago.

Buscar una AMI de pago mediante la consola

Para buscar una AMI de pago mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija AMIs.
3. Elija Imágenes públicas como primer filtro.
4. En la barra de búsqueda, elija Alias de propietario, luego = y, a continuación, aws-marketplace.
5. Si sabe el código de producto, elija Código de producto, luego = e introduzca el código.

Busque una AMI de pago mediante AWS Marketplace

Para buscar una AMI de pago mediante AWS Marketplace

1. Abrir AWS Marketplace.
2. Introduzca el nombre del sistema operativo en el campo de búsqueda y, a continuación, elija el botón de búsqueda (lupa).
3. Para ampliar más los resultados, use una de las categorías o filtros.
4. Cada producto está etiquetado con su tipo, bien `AMI` o `Software as a Service`.

Buscar una AMI pagada mediante AWS CLI

Puede encontrar una AMI de pago utilizando el siguiente comando describe-images (AWS CLI).

```
aws ec2 describe-images
    --owners aws-marketplace
```

Este comando devuelve numerosos detalles que describen cada AMI, incluido el código de producto de una AMI de pago. El resultado de `describe-images` tiene una entrada para el código del producto como la siguiente:

```
"ProductCodes": [
    {
        "ProductCodeId": "product_code",
        "ProductCodeType": "marketplace"
    }
],
```

Si sabe el código de producto, puede filtrar los resultados por código de producto. Este ejemplo devuelve las AMI más recientes con el código de producto especificado.

```
aws ec2 describe-images
    --owners aws-marketplace \
    --filters "Name=product-code,Values=product_code" \
    --query "sort_by(Images, &CreationDate)[-1].[ImageId]"
```

Buscar una AMI pagada mediante Tools for Windows PowerShell

Puede encontrar una AMI de pago utilizando el siguiente comando Get-EC2Image.

```
PS C:\> Get-EC2Image -Owner aws-marketplace
```

El resultado para una AMI de pago incluye el código de producto.

```
ProductCodeId           ProductCodeType
-------------           ---------------
product_code            marketplace
```

Si sabe el código de producto, puede filtrar los resultados por código de producto. Este ejemplo devuelve las AMI más recientes con el código de producto especificado.

```
PS C:\> (Get-EC2Image -Owner aws-marketplace -Filter @{"Name"="product-
code";"Value"="product_code"} | sort CreationDate -Descending | Select-Object -First
 1).ImageId
```

Comprar una AMI de pago

Debe registrarse para (comprar) una AMI de pago antes de iniciar una instancia con la AMI.

Por lo general, el vendedor de la AMI de pago le presenta información acerca de la AMI, incluido su precio y un enlace donde puede comprarla. Cuando hace clic en el enlace, se le pide que inicie sesión en AWS primero y, a continuación, puede comprar la AMI.

Comprar una AMI de pago mediante la consola

Puede comprar una AMI de pago utilizando el launch wizard de Amazon EC2. Para obtener más información, consulte iniciar una AWS Marketplace instancia.

Suscribirse a un producto mediante AWS Marketplace

Para utilizar AWS Marketplace, debe disponer de una cuenta de AWS. Para iniciar instancias desde los productos de AWS Marketplace, debe haberse registrado para utilizar el servicio de Amazon EC2 y haberse suscrito al producto desde el que inicia la instancia. Hay dos formas de suscribirse a los productos en AWS Marketplace:

- Sitio web de AWS Marketplace: puede iniciar el software preconfigurado rápidamente con la característica de implementación de un clic.
- Launch wizard de Amazon EC2: puede buscar una AMI y iniciar una instancia directamente desde el asistente. Para obtener más información, consulte iniciar una AWS Marketplace instancia.

Obtener el código de producto de una instancia

Puede recuperar el código del producto de AWS Marketplace de la instancia mediante los metadatos de instancia. Si la instancia tiene un código de producto, Amazon EC2 lo devuelve. Para obtener más información acerca de la recuperación de metadatos, consulte Recuperar metadatos de instancia.

Para recuperar el código de producto, utilice el siguiente comando para el sistema operativo de la instancia.

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/product-codes
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/product-codes
```

Windows

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/product-codes
```

Usar el soporte de pago

Amazon EC2 también ofrece a los desarrolladores soporte de software (o AMI derivadas). Los desarrolladores pueden crear productos de soporte para cuyo uso se puede registrar. Durante el registro para recibir el producto de soporte, el desarrollador le proporciona un código de producto que debe asociar a la AMI. Esto permite al desarrollador confirmar que la instancia tiene derecho a soporte. También garantiza que, cuando ejecute las instancias del producto, se le cobre según los términos que especifique el desarrollador.

> **Important**
>
> No puede usar un producto de soporte con instancias reservadas. Siempre pagará el precio que especifique el vendedor del producto de soporte.

Para asociar un código de producto con la AMI, use uno de los comandos siguientes, donde ami_id es el ID de la AMI y product_code es el código del producto:

- modify-image-attribute (AWS CLI)

```
aws ec2 modify-image-attribute --image-id ami_id --product-codes "product_code"
```

- Edit-EC2ImageAttribute (AWS Tools for Windows PowerShell)

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami_id -ProductCode product_code
```

Una vez establecido el atributo de código de producto, no se puede cambiar ni quitar.

Facturas para AMI pagada y soportadas

Al final de mes, recibirá un correo electrónico con la cantidad que se ha cobrado en la tarjeta de crédito por el uso de alguna AMI de pago o admitida durante el mes. Esta factura es independiente de la factura habitual de Amazon EC2. Para obtener más información, consulte Paying for products en la Guía del comprador de AWS Marketplace.

Administrar las suscripciones de AWS Marketplace

En el sitio web de AWS Marketplace, puede consultar los detalles de la suscripción, ver las instrucciones de uso del proveedor, administrar las suscripciones y mucho más.

Para consultar los detalles de las suscripciones

1. Inicie sesión en la AWS Marketplace.
2. Elija Su cuenta de Marketplace.
3. Elija Administrar las suscripciones de software.
4. Se muestra una lista de las suscripciones activas. Elija Instrucciones de uso para ver instrucciones específicas de uso del producto, por ejemplo, un nombre de usuario para conectarse a la instancia en ejecución.

Para cancelar una suscripción de AWS Marketplace

1. Asegúrese de que ha terminado cualquier instancia que esté en ejecución desde la suscripción.
   a. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
   b. En el panel de navegación, seleccione Instances (Instancia[s]).
   c. Seleccione la instancia y luego elija Estado de la instancia, Terminar instancia.
   d. Cuando se le indique que confirme, elija Terminar.
2. Inicie sesión en AWS Marketplace y elija Su cuenta de Marketplace y, a continuación, Administrar las suscripciones de software.
3. Elija Cancelar suscripción. Se le pide que confirme la cancelación.

> **Note**
>
> Después de cancelar la suscripción, ya no puede iniciar ninguna instancia desde esa AMI. Para volver a utilizar esa AMI, debe volver a suscribirse a ella, ya sea en el sitio

web de AWS Marketplace o a través del asistente de inicialización en la consola de Amazon EC2.

Ciclo de vida de AMI

Puede crear sus propias AMI, copiarlas, respaldarlas y conservarlas hasta que esté listo para darlas de baja o anular su registro.

Contenido

Creación de una AMI

Puede crear AMI de Linux o Windows que estén respaldadas por volúmenes de Amazon EBS. También puede crear AMI de Linux que estén respaldadas por volúmenes de almacén de instancias (las AMI de Windows no admiten el almacén de instancias para el dispositivo raíz). También puede usar Windows Sysprep para crear AMI de Windows.

Temas

Creación de una AMI basada en Amazon EBS

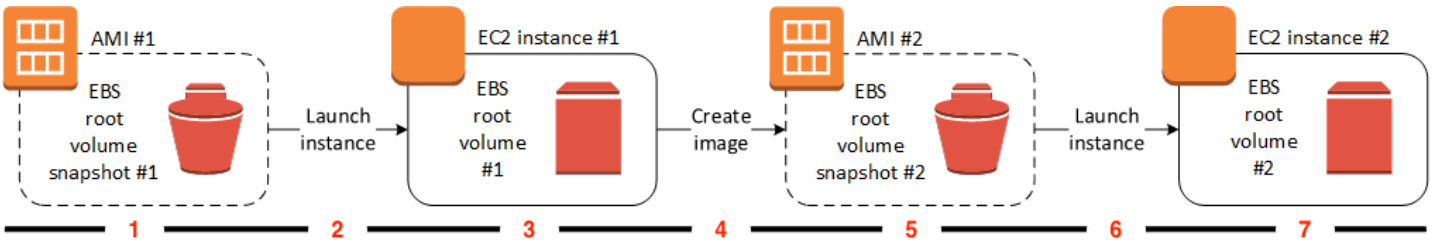
Para crear una AMI basada en Amazon EBS, comience desde una instancia que haya iniciado a partir de una AMI basada en Amazon EBS. Esta puede ser una AMI que haya obtenido del AWS Marketplace, una AMI que haya creado mediante AWS Server Migration Service o VM Import/Export o cualquier otra AMI a la que tenga acceso. Una vez que haya personalizado la instancia según sus necesidades, cree y registre una nueva AMI, que puede utilizar para iniciar nuevas instancias con dicha configuración personalizada.

Los procedimientos que se describen a continuación funcionan con instancias de Amazon EC2 respaldadas tanto por volúmenes de Amazon Elastic Block Store (Amazon EBS) cifrados (incluido el volumen raíz) como por volúmenes sin cifrar.

El proceso de creación de la AMI es diferente para las imágenes de tipo AMIs con respaldo en el almacén de instancias. Para obtener más información acerca de las diferencias entre las instancias respaldadas por Amazon EBS y las instancias respaldadas por el almacenamiento de instancias y sobre cómo determinar el tipo de dispositivo raíz para una instancia, consulte Almacenamiento para el dispositivo raíz. Para obtener más información acerca de la creación de una AMI basada en el almacén de instancias, consulte Crear una AMI de Linux con respaldo en el almacén de instancias.

Información general acerca de la creación de AMIs con el respaldo Amazon EBS

En el siguiente diagrama se resume el proceso de creación de una AMI basada en Amazon EBS a partir de una instancia de EC2 en ejecución: comience con una AMI existente, lance una instancia, personalícela, cree una nueva AMI a partir de ella y, finalmente, lance una instancia de la nueva AMI. Los números del diagrama coinciden con los números de la siguiente descripción.



1: AMI Nro. 1, comenzar con una AMI existente

Busque una AMI existente que sea similar a la AMI que desea crear. Esta puede ser una AMI que haya obtenido del AWS Marketplace, una AMI que haya creado mediante AWS Server Migration Service o VM Import/Export o cualquier otra AMI a la que tenga acceso. Personalizará esta AMI según sus necesidades.

En el diagrama, Instantánea del volumen raíz de EBS Nro. 1 indica que la AMI es una AMI basada en Amazon EBS y que la información sobre el volumen raíz se almacena en esta instantánea.

2: iniciar una instancia desde la AMI existente

La forma de configurar una AMI consiste en iniciar una instancia desde la AMI en la que desea basar la nueva AMI y, a continuación, personalizar la instancia (indicada en 3 en el diagrama). A continuación, creará una nueva AMI que incluya las personalizaciones (indicadas en 4 en el diagrama).

3: instancia de EC2 Nro. 1, personalizar la instancia

Conéctese a la instancia y personalícela. La nueva AMI incluirá estas personalizaciones.

Puede realizar cualquiera de las siguientes acciones sobre la instancia para personalizarla y que se ajuste a sus necesidades:

- Instalar software y aplicaciones.
- Copiar datos.
- Reducir el tiempo de inicio al eliminar los archivos temporales y desfragmentar el disco duro
- Adjuntar volúmenes de EBS adicionales.

4: Crear imagen

Cuando crea una AMI a partir de una instancia, Amazon EC2 apaga la instancia antes de crear la AMI para asegurarse de que todo lo que hay en la instancia está detenido y en un estado constante durante el proceso de creación. Si está seguro de que la instancia está en un estado coherente adecuado para la creación de una AMI, puede informar a Amazon EC2 de que no apague y reinicie la instancia. Algunos sistemas de archivos, como XFS, pueden pausar y reanudar la actividad, de forma que sea seguro crear la imagen sin tener que reiniciar la instancia.

Durante el proceso de creación de la AMI, Amazon EC2 crea instantáneas del volumen raíz de la instancia y de cualquier otro volumen de EBS asociado a la instancia. Se le cobra por las instantáneas hasta que anule el registro de la AMI y las elimine. Si alguno de los volúmenes adjuntos a la instancia está cifrado, la nueva AMI solo se inicia correctamente en instancias que admiten el cifrado de Amazon EBS.

Según el tamaño de los volúmenes, el proceso de creación de la AMI puede tardar varios minutos en completarse (a veces, hasta 24 horas). Resulta más eficiente crear instantáneas de los volúmenes antes de crear la AMI. De esta forma, solo es necesario crear pequeñas

instantáneas incrementales cuando se cree la AMI y, de esta manera, el proceso se completará más rápidamente (el tiempo total de creación de las instantáneas sigue siendo el mismo).

5: AMI Nro. 2, nueva AMI

Una vez completado el proceso, tendrá una nueva AMI y una instantánea (instantánea Nro. 2) creada desde el volumen raíz de la instancia. Si agrega volúmenes de almacén de instancias o volúmenes EBS a la instancia además del volumen de dispositivo raíz, la asignación de dispositivos de bloques de la nueva AMI contiene información relativa a esos volúmenes.

Amazon EC2 registra la AMI automáticamente.

6: iniciar una instancia desde una nueva AMI

Puede utilizar la nueva AMI para iniciar una instancia.

7: instancia de EC2 Nro. 2, nueva instancia

Cuando inicia una instancia con la nueva AMI, Amazon EC2 crea un nuevo volumen de EBS para el volumen raíz de la instancia mediante la instantánea. Si agregó volúmenes de almacén de instancias o volúmenes de EBS al personalizar la instancia, la asignación de dispositivos de bloques de la nueva AMI contendrá información relativa a esos volúmenes y las asignaciones de dispositivos de bloques de las instancias que lance desde la nueva AMI contendrán automáticamente información relativa a estos volúmenes. Los volúmenes de almacén de instancias especificados en la asignación de dispositivos de bloques de la nueva instancia son nuevos y no contienen ningún dato de los volúmenes de almacén de instancias de la instancia que usó para crear la AMI. Los datos en los volúmenes de EBS persisten. Para obtener más información, consulte Mapeos de dispositivos de bloques.

Cuando cree una nueva instancia desde una AMI respaldada por EBS, deberá inicializar tanto su volumen raíz como cualquier almacenamiento de EBS adicional antes de ponerla en producción. Para obtener más información, consulte Inicializar volúmenes de Amazon EBS en la Guía del usuario de Amazon EBS.

Creación de una AMI a partir de una instancia

Puede crear una AMI mediante la AWS Management Console o la línea de comandos.

Console

Para crear una AMI

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Seleccione la instancia desde la cual crear la AMI y, a continuación, elija Acciones, Imagen y plantillas, Crear imagen.

> **Tip**
>
> Si se deshabilita esta opción, la instancia no es una instancia con respaldo Amazon EBS.

4. En la página Crear imagen, especifique la siguiente información:

   a. En Nombre de la imagen, escriba un nombre único para la imagen, con un máximo de 127 caracteres.

   b. En Descripción de la imagen, ingrese una descripción opcional de la imagen con un máximo de 255 caracteres.

   c. En No reiniciar, mantenga desmarcada la casilla de verificación Habilitar (opción predeterminada) o selecciónela.

   - Si la opción Habilitar está desactivada en Sin reinicio, cuando Amazon EC2 cree la nueva AMI, reiniciará la instancia para que pueda tomar instantáneas de los volúmenes asociados mientras los datos estén en reposo para garantizar un estado coherente.
   - Si la opción Habilitar está activada en Sin reinicio, cuando Amazon EC2 cree la nueva AMI, no cerrará ni reiniciará la instancia.

   > **Warning**
   >
   > Si decide habilitar Sin reinicio, no podemos garantizar la integridad del sistema de archivos de la imagen creada.

   d. Volúmenes de instancia: puede modificar el volumen raíz, así como agregar más volúmenes de Amazon EBS y de almacén de instancias, de la siguiente manera:

i. El volumen raíz se define en la primera fila.

- A fin de cambiar el tamaño del volumen raíz, en Tamaño, introduzca el valor requerido.
- Si selecciona Eliminar al terminar, cuando termina la instancia creada con esta AMI, se elimina el volumen de EBS. Si borra Eliminar al terminar, cuando termina la instancia, no se elimina el volumen de EBS. Para obtener más información, consulte Conservación de los datos cuando se termina una instancia.

ii. Para agregar un volumen de EBS, elija Agregar volumen (lo que agrega una fila nueva). En Tipo de almacenamiento, elija EBS y rellene los campos de la fila. Cuando inicia una instancia desde la nueva AMI, los volúmenes adicionales se asocian de forma automática a la instancia. Los volúmenes vacíos se tienen que formatear y montar. Los volúmenes basados en una instantánea se deben montar.

iii. Para añadir un volumen de almacén de instancias, consulte Agregar volúmenes de almacén de instancias a una AMI. Cuando inicia una instancia desde la nueva AMI, los volúmenes adicionales se inicializan y se montan de forma automática. Estos volúmenes no contienen datos de los volúmenes de almacén de instancias de la instancia en ejecución en la que ha basado la AMI.

e. Etiquetas: puede etiquetar la AMI y las instantáneas con las mismas etiquetas o con etiquetas diferentes.

- Para etiquetar la AMI y las instantáneas con las mismas etiquetas, elija Etiquetar imagen e instantáneas juntas. Las mismas etiquetas se aplican a la AMI y a todas las instantáneas que se crean.
- Para etiquetar la AMI y las instantáneas con etiquetas diferentes, elija Etiquetar imagen e instantáneas por separado. Se aplican diferentes etiquetas a la AMI y a las instantáneas que se crean. Sin embargo, todas las instantáneas obtienen las mismas etiquetas; no puede etiquetar cada instantánea con una etiqueta diferente.

Para agregar una etiqueta, elija Add tag (Agregar etiqueta) y especifique la clave y el valor de la etiqueta. Repita este proceso para cada etiqueta.

f. Cuando lo tenga todo listo para crear la AMI, seleccione Create image (Crear imagen).

5. Para ver el estado de la AMI mientras se crea:

a. En el panel de navegación, elija AMI.

b. Establezca el filtro en De mi propiedad y busque la AMI en la lista.

   Al principio, el estado es `pending`, pero debe cambiar a `available` después de unos minutos.

6. (Opcional) Para ver la instantánea creada para la nueva AMI:

   a. Anote el ID de la AMI que encontró en el paso anterior.

   b. En el panel de navegación, elija Instantáneas.

   c. Establezca el filtro en De mi propiedad y, a continuación, busque la instantánea con el ID de la nueva AMI en la columna Descripción.

      Cuando se inicia una instancia desde esta AMI, Amazon EC2 usa esta instantánea para crear su volumen de dispositivo raíz.

AWS CLI

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

- create-image (AWS CLI)
- New-EC2Image (AWS Tools for Windows PowerShell)

Crear una AMI de Linux desde una instantánea

Si tiene una instantánea del volumen de dispositivo raíz de una instancia, puede crear una AMI de Linux a partir de esta instantánea con la AWS Management Console o la línea de comandos. Esta característica no está disponible actualmente para instancias de Windows.

Console

Para crear una AMI a partir de una instantánea

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instantáneas.
3. Seleccione la instantánea desde la cual crear la AMI y, a continuación, elija Acciones, Crear imagen a partir de una instantánea.
4. En la página Crear imagen a partir de una instantánea, especifique la siguiente información:

a. En Nombre de imagen, ingrese un nombre descriptivo para la imagen.

b. En Descripción, ingrese una breve descripción de la imagen.

c. En Arquitectura, elija la arquitectura de la imagen. Elija i386 para 32 bits, x86_64 para 64 bits, arm64 para ARM de 64 bits o x86_64 para macOS de 64 bits.

d. En Nombre del dispositivo raíz, ingrese el nombre de dispositivo que utilizará para el volumen de dispositivo raíz. Para obtener más información, consulte Nombres de dispositivos en las instancias de Amazon EC2.

e. En Tipo de virtualización, elija el tipo de virtualización que utilizarán las instancias iniciadas desde esta AMI. Para obtener más información, consulte Tipos de virtualización de AMI.

f. (Solo para virtualización paravirtual) En ID de kernel, seleccione el kernel del sistema operativo de la imagen. Si utiliza una instantánea del volumen de dispositivo raíz de una instancia, seleccione el mismo ID de kernel que la instancia original. Si no está seguro, utilice el kernel predeterminado.

g. (Solo para virtualización paravirtual) En ID de disco RAM, seleccione el disco RAM de la imagen. Si seleccionó un kernel específico, es posible que tenga que seleccionar un disco RAM específico con los controladores compatibles.

h. En Modo de arranque, elija el modo de arranque de la imagen o elija Usar valor predeterminado para que, cuando se inicie una instancia con esta AMI, lo haga con el modo de arranque compatible con el tipo de instancia. Para obtener más información, consulte Establezca el modo de arranque de una AMI.

i. (Opcional) En la sección Asignación de dispositivos de bloques, personalice el volumen raíz y agregue más volúmenes de datos.

   Para cada volumen, puede especificar el tamaño, el tipo, las características de rendimiento, el comportamiento de la eliminación al momento de la terminación y el estado de cifrado. Para el volumen raíz, el tamaño no puede ser menor que el tamaño de la instantánea. Para el tipo de volumen, el volumen SSD de uso general `gp3` es la opción predeterminada.

j. (Opcional) En Etiquetas, puede agregar una o más etiquetas a la nueva AMI. Para agregar una etiqueta, elija Agregar etiqueta y especifique la clave y el valor de la etiqueta. Repita este proceso para cada etiqueta.

k. Cuando lo tenga todo listo para crear la AMI, seleccione Crear imagen.

AWS CLI

Para crear una AMI a partir de una instantánea mediante la línea de comando

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

- register-image (CLI de AWS)
- Register-EC2Image (AWS Tools for Windows PowerShell)

Cómo iniciar una instancia desde la AMI que ha creado

Puede iniciar una instancia desde la AMI que ha creado a partir de una instancia o instantánea.

Para iniciar una instancia desde la AMI

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Images (Imágenes), elija AMIs.
3. Establezca el filtro en De mi propiedad y seleccione la AMI.
4. Elija Iniciar instancia desde una AMI.
5. Acepte los valores predeterminados o especifique valores personalizados en el asistente de inicialización de instancias. Para obtener más información, consulte Lance una instancia con el nuevo asistente de inicialización de instancias.

Crear una AMI de Linux con respaldo en el almacén de instancias

La AMI que se especifica cuando se inicia una instancia determina el tipo de volumen del dispositivo raíz.

Para crear una AMI de Linux con respaldo en el almacén de instancias, comience desde una instancia que haya iniciado a partir de una AMI de Linux existente con respaldo en el almacén de instancias. Una vez que haya personalizado la instancia según sus necesidades, agrupe el volumen y registre una nueva AMI, que puede utilizar para iniciar nuevas instancias con dicha configuración personalizada.

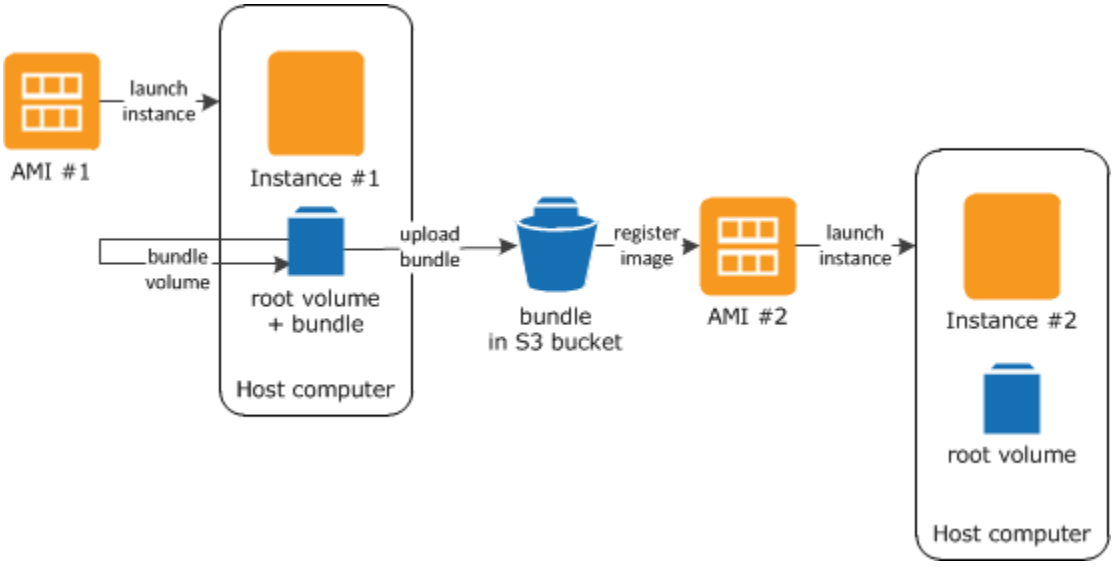
No puede crear una AMI de Windows que esté respaldada por el almacén de instancias, ya que las AMI de Windows no admiten el almacén de instancias para el dispositivo raíz.

> **Important**
>
> Sólo los siguientes tipos de instancia admiten un volumen de almacén de instancia como dispositivo raíz: C1, C3, D2, I2, M1, M2, M3, R3 y X1.

El proceso de creación de la AMI es diferente para las AMI con respaldo en Amazon EBS. Para obtener más información acerca de las diferencias entre las instancias respaldadas por Amazon EBS y las instancias con respaldo en el almacenamiento de la instancia y sobre cómo determinar el tipo de dispositivo raíz para una instancia, consulte Almacenamiento para el dispositivo raíz. Si necesita crear una AMI respaldada por Amazon EBS, consulte Creación de una AMI basada en Amazon EBS.

Información general acerca del proceso de creación de las AMI con respaldo en el almacenamiento de la instancia

En el siguiente diagrama se resume el proceso de creación de una AMI desde una instancia con respaldo en el almacén de instancias.



En primer lugar, lance una instancia desde una AMI que sea similar a la AMI que desea crear. Puede conectarse a la instancia y personalizarla. Cuando la instancia esté configurada como desea, puede agruparla. El proceso de agrupación tarda unos minutos en completarse. Una vez se haya completo el proceso, tiene un paquete formado por un manifiesto de imágenes (`image.manifest.xml`) y archivos (`image.part.xx`) que contienen una plantilla para el volumen raíz. A continuación, cargue el paquete al bucket de Amazon S3 y registre la AMI.

> **Note**
>
> Para cargar objetos en un bucket de S3 para la AMI de Linux respaldada por el almacén de instancias, las ACL deben estar habilitadas para el bucket. De lo contrario, Amazon EC2 no podrá configurar las ACL en los objetos que se van a cargar. Si el bucket de destino utiliza la configuración impuesta por el propietario del bucket para la propiedad de objetos de S3, esto no funcionará porque las ACL están deshabilitadas. Para obtener más información, consulte Control de la propiedad de objetos cargados mediante la propiedad de objetos de S3.

Cundo inicia una instancia utilizando la nueva AMI, se crea el volumen raíz de la instancia con el paquete que cargó en Amazon S3. El espacio de almacenamiento que utiliza el paquete en Amazon S3 genera cargos a la cuenta hasta que lo elimine. Para obtener más información, consulte Anular el registro de (eliminar) una AMI.

Si añade volúmenes de almacén de instancias a la instancia además del volumen de dispositivo raíz, la asignación de dispositivos de bloques de la nueva AMI contiene información relativa a estos volúmenes y los mapeos de dispositivos de bloques de las instancias que lance desde la nueva AMI contienen automáticamente información relativa a estos volúmenes. Para obtener más información, consulte Mapeos de dispositivos de bloques.

Requisitos previos

Antes de poder crear una AMI, debe ejecutar las siguientes tareas:

- Instalación de las herramientas de la AMI. Para obtener más información, consulte Configurar las herramientas de la AMI.
- Instale la AWS CLI. Para obtener más información, consulte Instalación de la AWS Command Line Interface.
- Asegúrese de tener un bucket de S3 para el paquete y de que su bucket tenga las ACL habilitadas. Para obtener más información sobre la configuración de las ACL, consulte Configuración de la ACL.
  - Para crear un bucket de S3 con la AWS Management Console, abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/ S3 y elija Crear bucket.
  - Para crear un bucket de S3 con la AWS CLI, puede utilizar el comando mb. Si la versión instalada de las herramientas de AMI es la 1.5.18 o posterior, también puede usar el comando `ec2-upload-bundle` para crear el bucket de S3. Para obtener más información, consulte ec2-upload-bundle.

- Asegúrese de tener el ID de la cuenta de AWS. Para obtener más información, consulte Visualización de identificadores de la Cuenta de AWS en la Guía de referencia de la Administración de cuentas de AWS.
- Asegúrese de tener credenciales para utilizar el AWS CLI. Para más información, consulte Prácticas recomendadas para cuentas de AWS en la Guía de referencia de AWS Account Management.
- Asegúrese de tener un certificado X.509 y su correspondiente clave privada.
  - Si necesita crear un certificado X.509, consulte Gestionar certificados de firma. El certificado X.509 y la clave privada se utilizan para cifrar y descifrar la AMI.
  - [China (Pekín)] Utilice el certificado `$EC2_AMITOOL_HOME/etc/ec2/amitools/cert-ec2-cn-north-1.pem`.
  - [AWS GovCloud (EE. UU. Oeste)] Utilice el certificado `$EC2_AMITOOL_HOME/etc/ec2/amitools/cert-ec2-gov.pem`.
- Conéctese a la instancia y personalícela. Por ejemplo, puede instalar software y aplicaciones, copiar datos, eliminar archivos temporales y modificar la configuración de Linux.

Tareas

- Configurar las herramientas de la AMI
- Crear una AMI desde una instancia de Amazon Linux con respaldo en el almacén de instancias
- Crear una AMI desde una instancia de Ubuntu con respaldo en el almacén de instancias
- Convertir la AMI con respaldo en el almacén de instancias a una AMI respaldada por Amazon EBS

Configurar las herramientas de la AMI

Puede utilizar las herramientas para AMI para crear y administrar las AMIs de Linux con respaldo en el almacén de instancias. Para utilizar las herramientas, debe instalarlas en su instancia de Linux. Las herramientas de la AMI están disponibles como un archivo RPM o como un archivo .zip para distribuciones Linux que no admiten RPM.

Para configurar las herramientas de la AMI con RPM

1. Instale Ruby utilizando el administrador de paquetes correspondiente de la distribución Linux, como, por ejemplo, yum. Por ejemplo:

```
[ec2-user ~]$ sudo yum install -y ruby
```

2. Descargue el archivo RPM utilizando una herramienta como wget o curl. Por ejemplo:

```
[ec2-user ~]$ wget https://s3.amazonaws.com/ec2-downloads/ec2-ami-tools.noarch.rpm
```

3. Ejecute el comando siguiente para verificar la firma del archivo RPM:

```
[ec2-user ~]$ rpm -K ec2-ami-tools.noarch.rpm
```

El comando anterior debería indicar que los hashes SHA1 y MD5 del archivo son `OK`. Si el comando indica que dichos hashes son `NOT OK`, utilice el siguiente comando para ver los hashes SHA1 y MD5 del encabezado del archivo:

```
[ec2-user ~]$ rpm -Kv ec2-ami-tools.noarch.rpm
```

A continuación, compare los hashes SHA1 y MD5 del encabezado del archivo con los siguientes hashes verificados de las herramientas de la AMI para confirmar la autenticidad del archivo:

- SHA1 del encabezado: a1f662d6f25f69871104e6a62187fa4df508f880
- MD5: 9faff05258064e2f7909b66142de6782

Si los hashes SHA1 y MD5 del encabezado del archivo coinciden con los hashes verificados de las herramientas de la AMI, continúe con el siguiente paso.

4. Instale el RPM utilizando el siguiente comando:

```
[ec2-user ~]$ sudo yum install ec2-ami-tools.noarch.rpm
```

5. Verifique la instalación de las herramientas de la AMI utilizando el comando ec2-ami-tools-version.

```
[ec2-user ~]$ ec2-ami-tools-version
```

> **Note**
>
> Si recibe un error de carga, como "cannot load such file -- ec2/amitools/version (LoadError)", complete el siguiente paso para añadir la ubicación de la instalación de las herramientas de la AMI a la ruta RUBYLIB.

6. (Opcional) Si recibió un error en el paso anterior, añada la ubicación de la instalación de las herramientas de la AMI a la ruta RUBYLIB.

   a. Ejecute el siguiente comando para determinar las rutas a añadir.

   ```
   [ec2-user ~]$ rpm -qil ec2-ami-tools | grep ec2/amitools/version
   /usr/lib/ruby/site_ruby/ec2/amitools/version.rb
   /usr/lib64/ruby/site_ruby/ec2/amitools/version.rb
   ```

   En el ejemplo anterior, el archivo que falta según el error de carga anterior se ubica en /usr/lib/ruby/site_ruby y en /usr/lib64/ruby/site_ruby.

   b. Añada las ubicaciones del paso anterior a la ruta RUBYLIB.

   ```
   [ec2-user ~]$ export RUBYLIB=$RUBYLIB:/usr/lib/ruby/site_ruby:/usr/lib64/ruby/site_ruby
   ```

   c. Verifique la instalación de las herramientas de la AMI utilizando el comando ec2-ami-tools-version.

   ```
   [ec2-user ~]$ ec2-ami-tools-version
   ```

Para configurar las herramientas de la AMI con el archivo .zip

1. Instale Ruby y descomprima el archivo utilizando el administrador de paquetes correspondiente de la distribución Linux, como, por ejemplo apt-get. Por ejemplo:

   ```
   [ec2-user ~]$ sudo apt-get update -y && sudo apt-get install -y ruby unzip
   ```

2. Descargue el archivo .zip utilizando una herramienta como wget o curl. Por ejemplo:

   ```
   [ec2-user ~]$ wget https://s3.amazonaws.com/ec2-downloads/ec2-ami-tools.zip
   ```

3. Descomprima los archivos en un directorio de instalación adecuado, como `/usr/local/ec2`.

```
[ec2-user ~]$ sudo mkdir -p /usr/local/ec2
$ sudo unzip ec2-ami-tools.zip -d /usr/local/ec2
```

   Observe que el archivo .zip contiene una carpeta ec2-ami-tools-*x*.*x*.*x*, donde *x*.*x*.*x* es el número de versión de las herramientas (por ejemplo, `ec2-ami-tools-1.5.7`).

4. Establezca la variable de entorno `EC2_AMITOOL_HOME` en el directorio de instalación de las herramientas. Por ejemplo:

```
[ec2-user ~]$ export EC2_AMITOOL_HOME=/usr/local/ec2/ec2-ami-tools-x.x.x
```

5. Agregue las herramientas a la variable de entorno `PATH`. Por ejemplo:

```
[ec2-user ~]$ export PATH=$EC2_AMITOOL_HOME/bin:$PATH
```

6. Puede verificar la instalación de las herramientas de la AMI utilizando el comando ec2-ami-tools-version.

```
[ec2-user ~]$ ec2-ami-tools-version
```

Gestionar certificados de firma

Ciertos comandos de las herramientas de la AMI requieren un certificado de firma (denominado también certificado X.509). Debe crear el certificado y, a continuación, cargarlo en AWS. Por ejemplo, puede utilizar una herramienta de terceros, como de OpenSSL, para crear el certificado.

Para crear un certificado de firma

1. Instale y configure OpenSSL.
2. Cree una clave privada mediante el comando `openssl genrsa` y guarde la clave resultante en un archivo `.pem`. Le recomendamos que cree una clave RSA de 2 048 o 4 096 bits.

```
openssl genrsa 2048 > private-key.pem
```

3. Genere un certificado mediante el comando `openssl req`.

```
openssl req -new -x509 -nodes -sha256 -days 365 -key private-key.pem -outform PEM -
out certificate.pem
```

Para cargar el certificado a AWS, utilice el comando upload-signing-certificate.

```
aws iam upload-signing-certificate --user-name user-name --certificate-body
 file://path/to/certificate.pem
```

Para ver la lista de certificados de un usuario, utilice el comando list-signing-certificates:

```
aws iam list-signing-certificates --user-name user-name
```

Para deshabilitar o volver a habilitar un certificado de firma para un usuario, utilice el comando update-signing-certificate. El siguiente comando deshabilita el certificado:

```
aws iam update-signing-certificate --certificate-id OFHPLP4ZULTHYPMSYEX7O4BEXAMPLE --
status Inactive --user-name user-name
```

Para eliminar un certificado, utilice el comando delete-signing-certificate:

```
aws iam delete-signing-certificate --user-name user-name --certificate-
id OFHPLP4ZULTHYPMSYEX7O4BEXAMPLE
```

Crear una AMI desde una instancia con respaldo en el almacén de instancias

Los siguientes procedimientos permiten crear una AMI con respaldo en el almacén de instancias AMI desde una instancia con respaldo en el almacén de instancias. Antes de comenzar, asegúrese de que ha leído los requisitos previos.

Temas

- Crear una AMI desde una instancia de Amazon Linux con respaldo en el almacén de instancias
- Crear una AMI desde una instancia de Ubuntu con respaldo en el almacén de instancias

Crear una AMI desde una instancia de Amazon Linux con respaldo en el almacén de instancias

En esta sección se describe la creación de una AMI desde una instancia de Amazon Linux. Los siguientes procedimientos podrían no funcionar para instancias que ejecutan otras distribuciones

Linux. Para conocer los procedimientos específicos para Ubuntu, consulte Crear una AMI desde una instancia de Ubuntu con respaldo en el almacén de instancias.

Para prepararse para utilizar las herramientas de la AMI (solo instancias HVM)

1. Las herramientas de la AMI requieren GRUB Legacy para arrancar correctamente. Utilice el siguiente comando para instalar GRUB:

```
[ec2-user ~]$ sudo yum install -y grub
```

2. Instale los paquetes de administración de particiones con el siguiente comando:

```
[ec2-user ~]$ sudo yum install -y gdisk kpartx parted
```

Para crear una AMI desde una instancia de Amazon Linux con respaldo en el almacén de instancias

En este procedimiento se presupone que ha satisfecho los requisitos previos que se indican en Requisitos previos.

En el siguiente ejemplo, reemplace cada *marcador de posición del usuario* con su propia información.

1. Cargue las credenciales en la instancia. Estas credenciales se utilizan para garantizar que solo usted y Amazon EC2 pueden obtener acceso a la AMI.

   a. Cree un directorio temporal en la instancia para las credenciales del modo siguiente:

   ```
   [ec2-user ~]$ mkdir /tmp/cert
   ```

   Esto le permite excluir las credenciales de la imagen creada.

   b. Copie el certificado X.509 y la clave privada correspondiente del equipo en el directorio `/tmp/cert` de la instancia utilizando una herramienta de copia segura como scp. La opción `-i` *`my-private-key`*`.pem` del comando scp es la clave privada que utiliza para conectarse a la instancia con SSH, no la clave privada X.509. Por ejemplo:

   ```
   you@your_computer:~ $ scp -i my-private-key.pem /
   path/to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem /
   path/to/cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem ec2-
   user@ec2-203-0-113-25.compute-1.amazonaws.com:/tmp/cert/
   ```

```
pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem  100%  717     0.7KB/s   00:00
cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem  100%  685     0.7KB/s   00:00
```

Puesto que se trata de archivos de texto sin formato, también puede abrir el certificado y la clave con un editor de texto y copiar el contenido en nuevos archivos en `/tmp/cert`.

2. Prepare el paquete a cargar en Amazon S3 ejecutando el comando ec2-bundle-vol desde dentro de la instancia. Asegúrese de especificar la opción `-e` para excluir el directorio en el que están almacenadas las credenciales. De forma predeterminada, el proceso de agrupación excluye los archivos que podrían contener información confidencial. Estos archivos incluyen `*.sw`, `*.swo`, `*.swp`, `*.pem`, `*.priv`, `*id_rsa*`, `*id_dsa*` `*.gpg`, `*.jks`, `*/.ssh/authorized_keys` y `*/.bash_history`. Para incluir todos estos archivos, use la opción `--no-filter`. Para incluir algunos de estos archivos, use la opción `--include`.

> **Important**
>
> De forma predeterminada, el proceso de agrupación de la AMI crea una serie de archivos comprimidos y cifrados en el directorio `/tmp` que representa el volumen raíz. Si no dispone de suficiente espacio libre en disco en `/tmp` para almacenar el paquete, necesita especificar una ubicación distinta para almacenar el paquete mediante la opción `-d` *`/path/to/bundle/storage`*. Algunas instancias tienen almacenamiento efímero montado en `/mnt` o en `/media/ephemeral0` que puede utilizar, o también puede crear, asociar y montar un nuevo volumen de Amazon EBS para almacenar el paquete. Para obtener más información, consulte Creación de un volumen de Amazon EBS en la Guía del usuario de Amazon EBS.

   a. Debe ejecutar el comando ec2-bundle-vol como raíz. Para la mayoría de comandos, puede utilizar sudo para obtener permisos elevados, pero en este caso debe ejecutar sudo -E su para mantener las variables de entorno.

      ```
      [ec2-user ~]$ sudo -E su
      ```

      Tenga en cuenta que la pregunta bash ahora le identifica como el usuario raíz y que el signo de dólar se ha sustituido por un hash tag, lo que indica que se encuentra en un shell raíz:

      ```
      [root ec2-user]#
      ```

b. Para crear el paquete de la AMI, ejecute el comando ec2-bundle-vol del modo siguiente:

```
[root ec2-user]# ec2-bundle-vol -k /tmp/cert/pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -c /tmp/cert/cert-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -u 123456789012 -r x86_64 -e /tmp/cert --
partition gpt
```

> **Note**
>
> En las regiones China (Pekín) y AWS GovCloud (EE. UU. Oeste), utilice el parámetro `--ec2cert` y especifique los certificados de acuerdo con lo indicado en los requisitos previos.

La creación de la imagen puede llevar unos minutos. Cuando el comando se complete, el directorio `/tmp` (o no predeterminado) contiene el paquete (`image.manifest.xml`, además de varios archivos `image.part.xx`).

c. Salga del shell raíz.

```
[root ec2-user]# exit
```

3. (Opcional) Para añadir más volúmenes de almacén de instancias, edite los mapeos de dispositivos de bloques del archivo `image.manifest.xml` de la AMI. Para obtener más información, consulte Mapeos de dispositivos de bloques.

a. Cree una copia de seguridad del archivo `image.manifest.xml`.

```
[ec2-user ~]$ sudo cp /tmp/image.manifest.xml /tmp/image.manifest.xml.bak
```

b. Reformatee el archivo `image.manifest.xml` para que sea más fácil de leer y editar.

```
[ec2-user ~]$ sudo xmllint --format /tmp/image.manifest.xml.bak > /tmp/
image.manifest.xml
```

c. Edite los mapeos de dispositivos de bloques en `image.manifest.xml` con un editor de texto. En el siguiente ejemplo se muestra una nueva entrada para el volumen de almacén de instancias `ephemeral1`.

> **Note**
>
> Para obtener una lista de los archivos excluidos, consulte ec2-bundle-vol.

```
<block_device_mapping>
  <mapping>
    <virtual>ami</virtual>
    <device>sda</device>
  </mapping>
  <mapping>
    <virtual>ephemeral0</virtual>
    <device>sdb</device>
  </mapping>
  <mapping>
    <virtual>ephemeral1</virtual>
    <device>sdc</device>
  </mapping>
  <mapping>
    <virtual>root</virtual>
    <device>/dev/sda1</device>
  </mapping>
</block_device_mapping>
```

d. Guarde el archivo `image.manifest.xml` y salga del editor de texto.

4. Para cargar el paquete a Amazon S3, ejecute el comando ec2-upload-bundle del modo siguiente.

```
[ec2-user ~]$ ec2-upload-bundle -b my-s3-bucket/bundle_folder/bundle_name -m /tmp/
image.manifest.xml -a your_access_key_id -s your_secret_access_key
```

> **Important**
>
> Para registrar la AMI en una región distinta a US East (N. Virginia), debe especificar tanto la región de destino con la opción `--region` como una ruta para el bucket que ya exista en la región de destino o bien una ruta para el bucket exclusiva que pueda crearse en la región de destino.

5. (Opcional) Una vez que el bucket se ha cargado en Amazon S3, puede eliminar el paquete del directorio `/tmp` de la instancia utilizando el siguiente comando rm:

```
[ec2-user ~]$ sudo rm /tmp/image.manifest.xml /tmp/image.part.* /tmp/image
```

> **Important**
>
> Si ha especificado una ruta con la opción `-d` *`/path/to/bundle/storage`* en Step 2, utilice dicha ruta en lugar de `/tmp`.

6. Para registrar la AMI, ejecute el comando register-image del modo siguiente.

```
[ec2-user ~]$ aws ec2 register-image --image-location my-s3-
bucket/bundle_folder/bundle_name/image.manifest.xml --name AMI_name --
virtualization-type hvm
```

> **Important**
>
> Si ha especificado previamente una región para el comando ec2-upload-bundle, especifique la misma región de nuevo para este comando.

Crear una AMI desde una instancia de Ubuntu con respaldo en el almacén de instancias

En esta sección se describe la creación de una AMI desde una instancia de Ubuntu Linux con un volumen de almacén de instancias como volumen raíz. Los siguientes procedimientos podrían no funcionar para instancias que ejecutan otras distribuciones Linux. Para obtener información sobre los procedimientos específicos de Amazon Linux, consulte Crear una AMI desde una instancia de Amazon Linux con respaldo en el almacén de instancias.

Para prepararse para utilizar las herramientas de la AMI (solo instancias HVM)

Las herramientas de la AMI requieren GRUB Legacy para arrancar correctamente. No obstante, Ubuntu está configurado para utilizar GRUB 2. Debe verificar si la instancia utiliza GRUB Legacy y, si no fuera así, necesita instalarlo y configurarlo.

Las instancias HVM también requieren la instalación de herramientas de particiones para que las herramientas de la AMI funcionen correctamente.

1. GRUB Legacy (versión 0.9*x* o inferior) debe estar instalado en la instancia. Verifique si dispone de GRUB Legacy e instálelo si fuera necesario.

   a. Verifique la versión de la instalación de GRUB.

   ```
   ubuntu:~$ grub-install --version
   grub-install (GRUB) 1.99-21ubuntu3.10
   ```

   En este ejemplo, la versión de GRUB es superior a la 0.9*x*, por lo que debe instalarse GRUB Legacy. Continúe en Step 1.b. Si ya dispone de GRUB Legacy, puede pasar a Step 2.

   b. Instale el paquete `grub` utilizando el siguiente comando.

   ```
   ubuntu:~$ sudo apt-get install -y grub
   ```

2. Instale los siguientes paquetes de administración de particiones con el administrador de paquetes de la distribución.

   - `gdisk` (algunas distribuciones llaman a este paquete `gptfdisk`)
   - `kpartx`
   - `parted`

   Utilice el siguiente comando.

   ```
   ubuntu:~$ sudo apt-get install -y gdisk kpartx parted
   ```

3. Verifique los parámetros del kernel de la instancia.

   ```
   ubuntu:~$ cat /proc/cmdline
   BOOT_IMAGE=/boot/vmlinuz-3.2.0-54-virtual root=UUID=4f392932-ed93-4f8f-
   aee7-72bc5bb6ca9d ro console=ttyS0 xen_emul_unplug=unnecessary
   ```

   Observe las opciones que siguen a los parámetros del kernel y del dispositivo raíz: `ro`, `console=ttyS0` y `xen_emul_unplug=unnecessary`. Sus opciones pueden ser diferentes.

4. Verifique las entradas de kernel en `/boot/grub/menu.lst`.

   ```
   ubuntu:~$ grep ^kernel /boot/grub/menu.lst
   kernel  /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs ro console=hvc0
   ```

```
kernel  /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs ro single
kernel  /boot/memtest86+.bin
```

Tenga en cuenta que el parámetro `console` apunta a `hvc0` en lugar de a `ttyS0` y que falta el parámetro `xen_emul_unplug=unnecessary`. De nuevo, sus opciones pueden ser diferentes.

5. Edite el archivo `/boot/grub/menu.lst` con el editor de texto que prefiera (por ejemplo, vim o nano) para cambiar la consola y añadir los parámetros que identificó anteriormente a las entradas de arranque.

```
title           Ubuntu 12.04.3 LTS, kernel 3.2.0-54-virtual
root            (hd0)
kernel          /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs
 ro console=ttyS0 xen_emul_unplug=unnecessary
initrd          /boot/initrd.img-3.2.0-54-virtual

title           Ubuntu 12.04.3 LTS, kernel 3.2.0-54-virtual (recovery mode)
root            (hd0)
kernel          /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs ro
 single console=ttyS0 xen_emul_unplug=unnecessary
initrd          /boot/initrd.img-3.2.0-54-virtual

title           Ubuntu 12.04.3 LTS, memtest86+
root            (hd0)
kernel          /boot/memtest86+.bin
```

6. Verifique que las entradas de kernel contengan ahora los parámetros correctos.

```
ubuntu:~$ grep ^kernel /boot/grub/menu.lst
kernel  /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs ro console=ttyS0
 xen_emul_unplug=unnecessary
kernel  /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs ro single
 console=ttyS0 xen_emul_unplug=unnecessary
kernel  /boot/memtest86+.bin
```

7. [Solo para Ubuntu 14.04 y posterior] A partir de Ubuntu 14.04, las AMI de Ubuntu con respaldo en el almacén de instancias utilizan una tabla de partición GPT y una partición EFI independiente montada en `/boot/efi`. El comando ec2-bundle-vol no agrupará esta partición de arranque, por lo que necesita comentar la entrada `/etc/fstab` para la partición EFI tal y como se muestra en el siguiente ejemplo.

```
LABEL=cloudimg-rootfs   /        ext4   defaults        0 0
```

```
#LABEL=UEFI     /boot/efi       vfat    defaults        0 0
/dev/xvdb       /mnt    auto    defaults,nobootwait,comment=cloudconfig 0       2
```

Para crear una AMI desde una instancia de Ubuntu con respaldo en el almacén de instancias

En este procedimiento se presupone que ha satisfecho los requisitos previos que se indican en Requisitos previos.

En el siguiente ejemplo, reemplace cada *marcador de posición del usuario* con su propia información.

1. Cargue las credenciales en la instancia. Estas credenciales se utilizan para garantizar que solo usted y Amazon EC2 pueden obtener acceso a la AMI.

   a. Cree un directorio temporal en la instancia para las credenciales del modo siguiente:

   ```
   ubuntu:~$ mkdir /tmp/cert
   ```

   Esto le permite excluir las credenciales de la imagen creada.

   b. Copie el certificado X.509 y la clave privada del equipo en el directorio `/tmp/cert` de la instancia utilizando una herramienta de copia segura como scp. La opción `-i my-private-key.pem` del comando scp es la clave privada que utiliza para conectarse a la instancia con SSH, no la clave privada X.509. Por ejemplo:

   ```
   you@your_computer:~ $ scp -i my-private-key.pem /
   path/to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem /
   path/to/cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem ec2-
   user@ec2-203-0-113-25.compute-1.amazonaws.com:/tmp/cert/
   pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem  100%  717     0.7KB/s   00:00
   cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem  100%  685     0.7KB/s   00:00
   ```

   Puesto que se trata de archivos de texto sin formato, también puede abrir el certificado y la clave con un editor de texto y copiar el contenido en nuevos archivos en `/tmp/cert`.

2. Prepare el paquete a cargar en Amazon S3 ejecutando el comando ec2-bundle-vol desde la instancia. Asegúrese de especificar la opción `-e` para excluir el directorio en el que están almacenadas las credenciales. De forma predeterminada, el proceso de agrupación excluye los archivos que podrían contener información confidencial. Estos archivos incluyen `*.sw`, `*.swo`,

`*.swp`, `*.pem`, `*.priv`, `*id_rsa*`, `*id_dsa*` `*.gpg`, `*.jks`, `*/.ssh/authorized_keys` y `*/.bash_history`. Para incluir todos estos archivos, use la opción `--no-filter`. Para incluir algunos de estos archivos, use la opción `--include`.

> **Important**
>
> De forma predeterminada, el proceso de agrupación de la AMI crea una serie de archivos comprimidos y cifrados en el directorio `/tmp` que representa el volumen raíz. Si no dispone de suficiente espacio libre en disco en `/tmp` para almacenar el paquete, necesita especificar una ubicación distinta para almacenar el paquete mediante la opción `-d` *`/path/to/bundle/storage`*. Algunas instancias tienen almacenamiento efímero montado en `/mnt` o en `/media/ephemeral0` que puede utilizar, o también puede crear, asociar y montar un nuevo volumen de Amazon EBS para almacenar el paquete. Para obtener más información, consulte Creación de un volumen de Amazon EBS en la Guía del usuario de Amazon EBS.

a. Debe ejecutar el comando ec2-bundle-vol necesario como raíz. Para la mayoría de comandos, puede utilizar sudo para obtener permisos elevados, pero en este caso debe ejecutar sudo -E su para mantener las variables de entorno.

```
ubuntu:~$ sudo -E su
```

Tenga en cuenta que la pregunta bash ahora le identifica como el usuario raíz y que el signo de dólar se ha sustituido por un hash tag, lo que indica que se encuentra en un shell raíz:

```
root@ubuntu:#
```

b. Para crear el paquete de la AMI, ejecute el comando ec2-bundle-vol del modo siguiente.

```
root@ubuntu:# ec2-bundle-vol -k /tmp/cert/pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -c /tmp/cert/cert-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -u your_aws_account_id -r x86_64 -e /tmp/
cert --partition gpt
```

> **Important**
>
> Para las instancias HVM de Ubuntu 14.04 y posterior, añada la marca `--partition mbr` para agrupar las instrucciones de arranque correctamente; de lo contrario, la AMI recién creada no arrancará.

La creación de la imagen puede llevar unos minutos. Cuando el comando se complete, el directorio `tmp` contiene el paquete (`image.manifest.xml`, además de varios archivos `image.part.`*`xx`*).

c. Salga del shell raíz.

```
root@ubuntu:# exit
```

3. (Opcional) Para añadir más volúmenes de almacén de instancias, edite los mapeos de dispositivos de bloques del archivo `image.manifest.xml` de la AMI. Para obtener más información, consulte Mapeos de dispositivos de bloques.

   a. Cree una copia de seguridad del archivo `image.manifest.xml`.

   ```
   ubuntu:~$ sudo cp /tmp/image.manifest.xml /tmp/image.manifest.xml.bak
   ```

   b. Reformatee el archivo `image.manifest.xml` para que sea más fácil de leer y editar.

   ```
   ubuntu:~$ sudo xmllint --format /tmp/image.manifest.xml.bak > /tmp/
   image.manifest.xml
   ```

   c. Edite los mapeos de dispositivos de bloques en `image.manifest.xml` con un editor de texto. En el siguiente ejemplo se muestra una nueva entrada para el volumen de almacén de instancias *`ephemeral1`*.

   ```
   <block_device_mapping>
     <mapping>
       <virtual>ami</virtual>
       <device>sda</device>
     </mapping>
     <mapping>
       <virtual>ephemeral0</virtual>
       <device>sdb</device>
   ```

```
    </mapping>
    <mapping>
      <virtual>ephemeral1</virtual>
      <device>sdc</device>
    </mapping>
    <mapping>
      <virtual>root</virtual>
      <device>/dev/sda1</device>
    </mapping>
  </block_device_mapping>
```

d. Guarde el archivo `image.manifest.xml` y salga del editor de texto.

4. Para cargar el paquete a Amazon S3, ejecute el comando ec2-upload-bundle del modo siguiente.

```
ubuntu:~$ ec2-upload-bundle -b my-s3-bucket/bundle_folder/bundle_name -m /tmp/
image.manifest.xml -a your_access_key_id -s your_secret_access_key
```

> **Important**
>
> Si tiene previsto registrar la AMI en una región distinta a US East (N. Virginia), debe especificar tanto la región de destino con la opción `--region` como una ruta para el bucket que ya exista en la región de destino o bien una ruta para el bucket exclusiva que pueda crearse en la región de destino.

5. (Opcional) Una vez que el bucket se ha cargado en Amazon S3, puede eliminar el paquete del directorio `/tmp` de la instancia utilizando el siguiente comando rm:

```
ubuntu:~$ sudo rm /tmp/image.manifest.xml /tmp/image.part.* /tmp/image
```

> **Important**
>
> Si ha especificado una ruta con la opción `-d` */path/to/bundle/storage* en Step 2, utilice la misma ruta a continuación, en lugar de `/tmp`.

6. Para registrar la AMI, ejecute el comando register-image de la AWS CLI del modo siguiente.

```
ubuntu:~$ aws ec2 register-image --image-location my-s3-
bucket/bundle_folder/bundle_name/image.manifest.xml --name AMI_name --
virtualization-type hvm
```

> **Important**
>
> Si ha especificado previamente una región para el comando ec2-upload-bundle, especifique la misma región de nuevo para este comando.

7. [Ubuntu 14.04 y posterior] Elimine el comentario de la entrada EFI en `/etc/fstab`; de lo contrario, la instancia en ejecución no podrá reiniciarse.

Convertir la AMI con respaldo en el almacén de instancias a una AMI respaldada por Amazon EBS

Puede convertir una AMI de Linux con respaldo en el almacén de instancias de la que sea propietario a una AMI de Linux respaldada por Amazon EBS.

> **Important**
>
> No puede convertir una AMI que no le pertenece.

Para convertir una AMI con respaldo en el almacén de instancias a una AMI respaldada por Amazon EBS

1. Lance una instancia de Amazon Linux desde una AMI respaldada por Amazon EBS. Para obtener más información, consulte Lance una instancia con el nuevo asistente de inicialización de instancias. Las instancias de Amazon Linux tienen las herramientas de la AMI y la AWS CLI preinstaladas.
2. Cargue la clave privada X.509 que utilizó para agrupar la AMI con respaldo en el almacén de instancias a la instancia. Esta clave se utiliza para garantizar que solo usted y Amazon EC2 pueden obtener acceso a la AMI.

   a. Cree un directorio temporal en la instancia para la clave privada X.509 del modo siguiente:

   ```
   [ec2-user ~]$ mkdir /tmp/cert
   ```

b. Copie la clave privada X.509 del equipo en el directorio `/tmp/cert` de la instancia utilizando una herramienta de copia segura como scp. El parámetro *my-private-key* del siguiente comando es la clave privada que utiliza para conectarse a la instancia con SSH. Por ejemplo:

```
you@your_computer:~ $ scp -i my-private-key.pem /
path/to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem ec2-
user@ec2-203-0-113-25.compute-1.amazonaws.com:/tmp/cert/
pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem  100%  717     0.7KB/s   00:00
```

3. Configurar las variables de entorno para usar el AWS CLI. Para obtener más información, consulte la sección Creación de un par de claves.

   a. (Recomendado) Configure las variables de entorno para la clave de acceso, la clave secreta y el token de acceso de AWS.

```
[ec2-user ~]$ export AWS_ACCESS_KEY_ID=your_access_key_id
[ec2-user ~]$ export AWS_SECRET_ACCESS_KEY=your_secret_access_key
[ec2-user ~]$ export AWS_SESSION_TOKEN=your_session_token
```

   b. Configure las variables de entorno para la clave de acceso y la clave secreta de AWS.

```
[ec2-user ~]$ export AWS_ACCESS_KEY_ID=your_access_key_id
[ec2-user ~]$ export AWS_SECRET_ACCESS_KEY=your_secret_access_key
```

4. Prepare un volumen de Amazon Elastic Block Store (Amazon EBS) para la nueva AMI.

   a. Cree un volumen de EBS vacío en la misma zona de disponibilidad que la instancia con el comando create-volume. Observe el ID de volumen en el resultado del comando.

> **Important**
>
> Este volumen de EBS debe tener el mismo tamaño o un tamaño mayor que el del volumen raíz del almacén de instancias original.

```
[ec2-user ~]$ aws ec2 create-volume --size 10 --region us-west-2 --
availability-zone us-west-2b
```

b. Asocie el volumen a la instancia respaldada por Amazon EBS utilizando el comando attach-volume.

```
[ec2-user ~]$ aws ec2 attach-volume --volume-id volume_id --instance-
id instance_id --device /dev/sdb --region us-west-2
```

5. Cree una carpeta para el paquete.

```
[ec2-user ~]$ mkdir /tmp/bundle
```

6. Descargue el paquete para la AMI basada en almacén de instancias en `/tmp/bundle` utilizando el comando ec2-download-bundle.

```
[ec2-user ~]$ ec2-download-bundle -b my-s3-bucket/bundle_folder/bundle_name -m
 image.manifest.xml -a $AWS_ACCESS_KEY_ID -s $AWS_SECRET_ACCESS_KEY --privatekey /
path/to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -d /tmp/bundle
```

7. Reconstituya el archivo de imagen desde el paquete utilizando el comando ec2-unbundle.

a. Cambie los directorios a la carpeta del paquete.

```
[ec2-user ~]$ cd /tmp/bundle/
```

b. Ejecute el comando ec2-unbundle.

```
[ec2-user bundle]$ ec2-unbundle -m image.manifest.xml --privatekey /path/to/pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem
```

8. Copie los archivos de la imagen desagrupada al nuevo volumen de EBS.

```
[ec2-user bundle]$ sudo dd if=/tmp/bundle/image of=/dev/sdb bs=1M
```

9. Sondee el volumen por si existiera alguna partición nueva sin agrupar.

```
[ec2-user bundle]$ sudo partprobe /dev/sdb1
```

10. Muestre los dispositivos de bloques para encontrar el nombre de dispositivo a montar.

```
[ec2-user bundle]$ lsblk
NAME         MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
/dev/sda    202:0    0   8G  0 disk
```

```
##/dev/sda1 202:1    0   8G  0 part /
/dev/sdb    202:80   0  10G  0 disk
##/dev/sdb1 202:81   0  10G  0 part
```

En este ejemplo, la partición a montar es `/dev/sdb1`, pero el nombre de dispositivo probablemente será diferente. Si el volumen no está particionado, el dispositivo a montar será similar a `/dev/sdb` (sin el dígito final de la partición del dispositivo).

11. Cree un punto de montaje para el nuevo volumen de EBS y monte el volumen.

```
[ec2-user bundle]$ sudo mkdir /mnt/ebs
[ec2-user bundle]$ sudo mount /dev/sdb1 /mnt/ebs
```

12. Abra el archivo `/etc/fstab` del volumen de EBS con el editor de texto que prefiera (por ejemplo vim o nano) y elimine cualquier entrada para volúmenes (efímeros) de almacén de instancias. Puesto que el volumen de EBS está montado en `/mnt/ebs`, el archivo `fstab` se ubica en `/mnt/ebs/etc/fstab`.

```
[ec2-user bundle]$ sudo nano /mnt/ebs/etc/fstab
#
LABEL=/     /           ext4    defaults,noatime  1   1
tmpfs       /dev/shm    tmpfs   defaults        0   0
devpts      /dev/pts    devpts  gid=5,mode=620  0   0
sysfs       /sys        sysfs   defaults        0   0
proc        /proc       proc    defaults        0   0
/dev/sdb        /media/ephemeral0       auto    defaults,comment=cloudconfig    0
     2
```

En este ejemplo se debe eliminar la última línea.

13. Desmonte el volumen y sepárelo de la instancia.

```
[ec2-user bundle]$ sudo umount /mnt/ebs
[ec2-user bundle]$ aws ec2 detach-volume --volume-id volume_id --region us-west-2
```

14. Cree una AMI desde el nuevo volumen de EBS del modo siguiente.

    a. Cree una instantánea del nuevo volumen de EBS.

```
[ec2-user bundle]$ aws ec2 create-snapshot --region us-west-2 --description
 "your_snapshot_description" --volume-id volume_id
```

b. Verifique que la instantánea esté completa.

```
[ec2-user bundle]$ aws ec2 describe-snapshots --region us-west-2 --snapshot-
id snapshot_id
```

c. Identifique la arquitectura del procesador, el tipo de virtualización y la imagen del kernel (`aki`) utilizados en la AMI original con el comando describe-images. Para este paso, necesita el ID de AMI de la AMI original con respaldo en el almacén de instancias.

```
[ec2-user bundle]$ aws ec2 describe-images --region us-west-2 --image-id ami-id
 --output text
IMAGES x86_64 amazon/amzn-ami-pv-2013.09.2.x86_64-s3 ami-8ef297be amazon
 available public machine aki-fc8f11cc instance-store paravirtual xen
```

En este ejemplo, la arquitectura es `x86_64` y el ID de la imagen del kernel es `aki-fc8f11cc`. Utilice estos valores en el siguiente paso. Si el resultado del comando anterior también muestra un `ari` ID, anótelo también.

d. Registre la nueva AMI con el ID de la instantánea del nuevo volumen de EBS y los valores del paso anterior. Si el resultado del comando anterior mostró un ID `ari`, inclúyalo en el siguiente comando con `--ramdisk-id` *`ari_id`*.

```
[ec2-user bundle]$ aws ec2 register-image --region us-west-2 --
name your_new_ami_name --block-device-mappings DeviceName=device-
name,Ebs={SnapshotId=snapshot_id} --virtualization-type paravirtual --
architecture x86_64 --kernel-id aki-fc8f11cc --root-device-name device-name
```

15. (Opcional) Una vez que haya probado que puede iniciar una instancia desde la nueva AMI, puede eliminar el volumen de EBS que creó para este procedimiento.

```
aws ec2 delete-volume --volume-id volume_id
```

Referencia de las herramientas para AMI

Puede utilizar los comandos de las herramientas para AMI para crear y administrar AMI de Linux con respaldo en el almacén de instancias. Para configurar las herramientas, consulte Configurar las herramientas de la AMI.

Para más información, consulte Prácticas recomendadas para cuentas de AWS en la Guía de referencia de AWS Account Management.

Comandos

- ec2-ami-tools-version
- ec2-bundle-image
- ec2-bundle-vol
- ec2-delete-bundle
- ec2-download-bundle
- ec2-migrate-manifest
- ec2-unbundle
- ec2-upload-bundle
- Opciones comunes de las herramientas para AMI

ec2-ami-tools-version

Descripción

Describe la versión de las herramientas para AMI.

Sintaxis

ec2-ami-tools-version

Salida

La información de la versión.

Ejemplo

El comando de este ejemplo muestra la información de versión de las herramientas para AMI que está usando.

```
[ec2-user ~]$ ec2-ami-tools-version
1.5.2 20071010
```

ec2-bundle-image

Descripción

Crea una AMI de Linux con respaldo en el almacén de instancias a partir de una imagen del sistema operativo creada en un archivo de bucle invertido.

Sintaxis

ec2-bundle-image -c *path* -k *path* -u *account* -i *path* [-d *path*] [--ec2cert *path*] [-r *architecture*] [--productcodes *code1*,*code2*,...] [-B *mapping*] [-p *prefix*]

Opciones

`-c, --cert` path

El archivo RSA de certificado de clave pública en código PEM del usuario.

Obligatorio: sí

`-k, --privatekey` path

La ruta de un archivo de clave RSA en código PEM. Deberá especificar esta clave para desempaquetar este paquete, por lo que conviene guardarla en un lugar seguro. Observe que la clave no tiene que estar registrada en la cuenta de AWS.

Obligatorio: sí

`-u, --user` account

El ID de la cuenta de AWS del usuario sin guiones.

Obligatorio: sí

`-i, --image` path

La ruta de la imagen que se agrupa.

Obligatorio: sí

`-d, --destination` path

El directorio en el que se crea la agrupación.

Valor predeterminado: `/tmp`

Obligatorio: no

`--ec2cert` path

La ruta del certificado de clave pública Amazon EC2 X.509 utilizado para cifrar el manifiesto de la imagen.

Las regiones `us-gov-west-1` y `cn-north-1` usan un certificado de clave pública no predeterminado y la ruta de dicho certificado debe especificarse con esta opción. La ruta del certificado varía según el método de instalación de las herramientas para AMI. En Amazon Linux, los certificados se encuentran en `/opt/aws/amitools/ec2/etc/ec2/amitools/`. Si ha instalado las herramientas para AMI desde el archivo ZIP o RPM de Configurar las herramientas de la AMI, los certificados se encuentran en `$EC2_AMITOOL_HOME/etc/ec2/amitools/`.

Obligatorio: solo para las regiones `us-gov-west-1` y `cn-north-1`.

`-r, --arch` architecture

Arquitectura de la imagen. Si no proporciona la arquitectura en la línea de comandos, se le pedirá cuando se inicie la agrupación.

Valores válidos: `i386` | `x86_64`

Requerido: No

`--productcodes` code1,code2,...

Los códigos de producto que se adjuntan a la imagen en el momento del registro, separados por comas.

Requerido: No

`-B, --block-device-mapping` mapping

Define el modo en que los dispositivos de bloques se exponen a una instancia de esta AMI si el tipo de instancia admite el dispositivo especificado.

Especifique una lista separada por comas de pares clave-valor, donde cada clave es un nombre virtual y cada valor es el nombre del dispositivo correspondiente. Entre los nombres virtuales se incluyen los siguientes:

- `ami`: el dispositivo del sistema de archivos raíz como lo ve la instancia

- `root`: el dispositivo del sistema de archivos raíz como lo ve el kernel
- `swap`: el dispositivo de intercambio como lo ve la instancia
- `ephemeralN`: el volumen N-simo del almacén de instancias

Requerido: No

`-p, --prefix` prefix

El prefijo del nombre de archivo para los archivos de AMI agrupados.

Valor predeterminado: el nombre del archivo de imagen. Por ejemplo, si la ruta de la imagen es `/var/spool/my-image/version-2/debian.img`, el prefijo predeterminado es `debian.img`.

Requerido: No

`--kernel` kernel_id

Obsoleto. Use register-image para establecer el kernel.

Requerido: No

`--ramdisk` ramdisk_id

Obsoleto. Use register-image para establecer el disco RAM si se requiere.

Requerido: no

Salida

Mensajes de estado que describen las fases y los estados del proceso de agrupación.

Ejemplo

En este ejemplo se crea una AMI agrupada a partir de una imagen del sistema operativo que se creó en un archivo de bucle invertido.

```
[ec2-user ~]$ ec2-bundle-image -k pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -c cert-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -u 111122223333 -i image.img -d bundled/ -r x86_64
Please specify a value for arch [i386]:
Bundling image file...
Splitting bundled/image.gz.crypt...
Created image.part.00
Created image.part.01
```

```
Created image.part.02
Created image.part.03
Created image.part.04
Created image.part.05
Created image.part.06
Created image.part.07
Created image.part.08
Created image.part.09
Created image.part.10
Created image.part.11
Created image.part.12
Created image.part.13
Created image.part.14
Generating digests for each part...
Digests generated.
Creating bundle manifest...
ec2-bundle-image complete.
```

ec2-bundle-vol

Descripción

Crea una AMI de Linux con respaldo en el almacén de instancias comprimiendo, cifrando y firmando una copia del volumen de dispositivo raíz para la instancia.

Amazon EC2 intenta heredar los códigos de producto, la configuración del kernel, la configuración del disco RAM y el mapeo de los dispositivos de bloques de la instancia.

De forma predeterminada, el proceso de agrupación excluye los archivos que podrían contener información confidencial. Estos archivos incluyen `*.sw`, `*.swo`, `*.swp`, `*.pem`, `*.priv`, `*id_rsa*`, `*id_dsa*` `*.gpg`, `*.jks`, `*/.ssh/authorized_keys` y `*/.bash_history`. Para incluir todos estos archivos, use la opción `--no-filter`. Para incluir algunos de estos archivos, use la opción `--include`.

Para obtener más información, consulte Crear una AMI de Linux con respaldo en el almacén de instancias.

Sintaxis

```
ec2-bundle-vol -c path -k path -u account [-d path] [--ec2cert path] [-
r architecture] [--productcodes code1,code2,...] [-B mapping] [--all] [-e
directory1,directory2,...] [-i file1,file2,...] [--no-filter] [-p prefix]
```

[-s *size*] [--[no-]inherit] [-v *volume*] [-P *type*] [-S *script*] [--fstab *path*] [--generate-fstab] [--grub-config *path*]

Opciones

`-c, --cert` path

El archivo RSA de certificado de clave pública en código PEM del usuario.

Obligatorio: sí

`-k, --privatekey` path

La ruta del archivo de clave RSA en código PEM del usuario.

Obligatorio: sí

`-u, --user` account

El ID de la cuenta de AWS del usuario sin guiones.

Obligatorio: sí

`-d, --destination` destination

El directorio en el que se crea la agrupación.

Valor predeterminado: `/tmp`

Obligatorio: no

`--ec2cert` path

La ruta del certificado de clave pública Amazon EC2 X.509 utilizado para cifrar el manifiesto de la imagen.

Las regiones `us-gov-west-1` y `cn-north-1` usan un certificado de clave pública no predeterminado y la ruta de dicho certificado debe especificarse con esta opción. La ruta del certificado varía según el método de instalación de las herramientas para AMI. En Amazon Linux, los certificados se encuentran en `/opt/aws/amitools/ec2/etc/ec2/amitools/`. Si ha instalado las herramientas para AMI desde el archivo ZIP o RPM de Configurar las herramientas de la AMI, los certificados se encuentran en `$EC2_AMITOOL_HOME/etc/ec2/amitools/`.

Obligatorio: solo para las regiones `us-gov-west-1` y `cn-north-1`.

`-r, --arch` architecture

La arquitectura de la imagen. Si no proporciona la arquitectura en la línea de comandos, se le pedirá que lo haga cuando se inicie la agrupación.

Valores válidos: `i386` | `x86_64`

Requerido: No

`--productcodes` code1,code2,...

Los códigos de producto que se adjuntan a la imagen en el momento del registro, separados por comas.

Requerido: No

`-B, --block-device-mapping` mapping

Define el modo en que los dispositivos de bloques se exponen a una instancia de esta AMI si el tipo de instancia admite el dispositivo especificado.

Especifique una lista separada por comas de pares clave-valor, donde cada clave es un nombre virtual y cada valor es el nombre del dispositivo correspondiente. Entre los nombres virtuales se incluyen los siguientes:

- `ami`: el dispositivo del sistema de archivos raíz como lo ve la instancia
- `root`: el dispositivo del sistema de archivos raíz como lo ve el kernel
- `swap`: el dispositivo de intercambio como lo ve la instancia
- `ephemeralN`: el volumen N-simo del almacén de instancias

Requerido: No

`-a, --all`

Agrupe todos los directorios, incluidos los que se encuentran en sistemas de archivos montados de forma remota.

Requerido: No

`-e, --exclude` directory1,directory2,...

Una lista de las rutas de directorio absolutas y los archivos que se excluyen de la operación de agrupación. Este parámetro sobrescribe la opción `--all`. Cuando se especifica la exclusión, los directorios y subdirectorios enumerados con el parámetro no se agruparán con el volumen.

Requerido: No

`-i, --include` file1,file2,...

Una lista de los archivos que se incluirán en la operación de agrupación. De lo contrario, los archivos especificados se excluirían de la AMI porque podrían contener información confidencial.

Requerido: No

`--no-filter`

Si se especifica, no excluiremos los archivos de la AMI porque podrían contener información confidencial.

Requerido: No

`-p, --prefix` prefix

El prefijo del nombre de archivo para los archivos de AMI agrupados.

Valor predeterminado: `image`

Requerido: No

`-s, --size` size

El tamaño, en MB (1024 * 1024 bytes), del archivo de imagen que se va a crear. El tamaño máximo es 10.240 MB.

Predeterminado: 10240

Requerido: No

`--[no-]inherit`

Indica si la imagen debería heredar los metadatos de la instancia (la opción predeterminada es heredar). La agrupación da error si habilita `--inherit` pero los metadatos de la instancia no son accesibles.

Requerido: No

`-v, --volume` volume

La ruta absoluta del volumen montado a partir del que se crea la agrupación.

Opción predeterminada: el directorio raíz (/)

Requerido: No

`-P, --partition` type

Indica si la imagen de disco debería usar una tabla de partición. Si no especifica un tipo de tabla de partición, la opción predeterminada es el tipo usado en el dispositivo de bloques del volumen, si se aplica; si no, la opción predeterminada es `gpt`.

Valores válidos: `mbr` | `gpt` | `none`

Requerido: No

`-S, --script` script

Un script de personalización que se ejecuta justo antes de la agrupación. El script debe esperar un argumento único, el punto de montaje del volumen.

Requerido: No

`--fstab` path

La ruta de fstab que se agrupa en la imagen. Si no se especifica, Amazon EC2 agrupa /etc/fstab.

Requerido: No

`--generate-fstab`

Agrupa el volumen usando fstab proporcionado por Amazon EC2.

Requerido: No

`--grub-config`

La ruta de un archivo de configuración de grub alternativo para agrupar en la imagen. De manera predeterminada, `ec2-bundle-vol` espera que `/boot/grub/menu.lst` o `/boot/grub/grub.conf` exista en la imagen clonada. Esta opción permite especificar la ruta de un archivo de configuración de grub alternativo que después se copiará sobre los predeterminados (si existen).

Requerido: No

`--kernel` kernel_id

Obsoleto. Use register-image para establecer el kernel.

Requerido: No

`--ramdisk`ramdisk_id

Obsoleto. Use register-image para establecer el disco RAM si se requiere.

Requerido: no

Salida

Mensajes de estado que describen las fases y los estados de la agrupación.

Ejemplo

En este ejemplo se crea una AMI agrupada comprimiendo, cifrando y firmando una instantánea del sistema de archivos raíz del equipo local.

```
[ec2-user ~]$ ec2-bundle-vol -d /mnt -k pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -c
 cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -u 111122223333 -r x86_64
  Copying / into the image file /mnt/image...
  Excluding:
       sys
       dev/shm
       proc
       dev/pts
       proc/sys/fs/binfmt_misc
       dev
       media
       mnt
       proc
       sys
       tmp/image
       mnt/img-mnt
  1+0 records in
  1+0 records out
  mke2fs 1.38 (30-Jun-2005)
  warning: 256 blocks unused.

  Splitting /mnt/image.gz.crypt...
  Created image.part.00
  Created image.part.01
  Created image.part.02
  Created image.part.03
  ...
  Created image.part.22
  Created image.part.23
  Generating digests for each part...
  Digests generated.
  Creating bundle manifest...
```

```
Bundle Volume complete.
```

ec2-delete-bundle

Descripción

Elimina la agrupación especificada del almacenamiento de Amazon S3. Después de eliminar una agrupación, no podrá iniciar instancias de la AMI correspondiente.

Sintaxis

ec2-delete-bundle -b *bucket* -a *access_key_id* -s *secret_access_key* [-t *token*] [--url *url*] [--region *region*] [--sigv *version*] [-m *path*] [-p *prefix*] [--clear] [--retry] [-y]

Opciones

`-b, --bucket` bucket

El nombre del bucket de Amazon S3 que contienen la AMI agrupada, seguido de un prefijo de ruta delimitado por '/' opcional

Obligatorio: sí

`-a, --access-key` access_key_id

El ID de la clave de acceso de AWS.

Obligatorio: sí

`-s, --secret-key` secret_access_key

La clave de acceso secreta de AWS.

Obligatorio: sí

`-t, --delegation-token` token

El token de delegación que se pasa junto con la solicitud de AWS. Para obtener más información, consulte Uso de credenciales de seguridad temporales.

Obligatorio: solo cuando se utilizan credenciales de seguridad temporales.

Valor predeterminado: el valor de la variable de entorno `AWS_DELEGATION_TOKEN` (si se ha establecido).

`--regionregion`

La región que se usa en la firma de la solicitud.

Valor predeterminado: `us-east-1`

Obligatorio: obligatorio si se usa la versión 4 de firma

`--sigvversion`

La versión de la firma que se usará cuando se firme la solicitud.

Valores válidos: `2` | `4`

Valor predeterminado: `4`

Requerido: No

`-m, --manifestpath`

La ruta del archivo de manifiesto.

Obligatorio: debe especificar `--prefix` o `--manifest`.

`-p, --prefix` prefix

El prefijo del nombre de archivo de la AMI asociada. Proporcione el prefijo completo. Por ejemplo, si el prefijo es image.img, use `-p image.img` y no `-p image`.

Obligatorio: debe especificar `--prefix` o `--manifest`.

`--clear`

Elimina el bucket de Amazon S3 si está vacío después de eliminar la agrupación especificada.

Requerido: No

`--retry`

Reintenta automáticamente en todos los errores de Amazon S3, hasta cinco veces por operación.

Requerido: No

`-y, --yes`

Supone automáticamente que la respuesta a todas las peticiones es afirmativa.

Requerido: no

Salida

Amazon EC2 muestra mensajes de estado que indican las fases y el estado del proceso de eliminación.

Ejemplo

En este ejemplo se elimina una agrupación de Amazon S3.

```
[ec2-user ~]$ ec2-delete-bundle -b DOC-EXAMPLE-BUCKET1 -a your_access_key_id -
s your_secret_access_key
Deleting files:
DOC-EXAMPLE-BUCKET1/image.manifest.xml
DOC-EXAMPLE-BUCKET1/image.part.00
DOC-EXAMPLE-BUCKET1/image.part.01
DOC-EXAMPLE-BUCKET1/image.part.02
DOC-EXAMPLE-BUCKET1/image.part.03
DOC-EXAMPLE-BUCKET1/image.part.04
DOC-EXAMPLE-BUCKET1/image.part.05
DOC-EXAMPLE-BUCKET1/image.part.06
Continue? [y/n]
y
Deleted DOC-EXAMPLE-BUCKET1/image.manifest.xml
Deleted DOC-EXAMPLE-BUCKET1/image.part.00
Deleted DOC-EXAMPLE-BUCKET1/image.part.01
Deleted DOC-EXAMPLE-BUCKET1/image.part.02
Deleted DOC-EXAMPLE-BUCKET1/image.part.03
Deleted DOC-EXAMPLE-BUCKET1/image.part.04
Deleted DOC-EXAMPLE-BUCKET1/image.part.05
Deleted DOC-EXAMPLE-BUCKET1/image.part.06
ec2-delete-bundle complete.
```

ec2-download-bundle

Descripción

Descarga las AMIs de Linux con respaldo en el almacén de instancias del almacén de Amazon S3.

Sintaxis

ec2-download-bundle -b *bucket* -a *access_key_id* -s *secret_access_key* -k *path* [--url *url*] [--region *region*] [--sigv *version*] [-m *file*] [-p *prefix*] [-d *directory*] [--retry]

Opciones

`-b, --bucket` bucket

El nombre del bucket de Amazon S3 en el que se encuentra la agrupación, seguido de un prefijo de ruta delimitado por '/' opcional.

Obligatorio: sí

`-a, --access-key` access_key_id

El ID de la clave de acceso de AWS.

Obligatorio: sí

`-s, --secret-key` secret_access_key

La clave de acceso secreta de AWS.

Obligatorio: sí

`-k, --privatekey` path

La clave privada usada para descifrar el manifiesto.

Obligatorio: sí

`--url` url

La URL del servicio Amazon S3.

Valor predeterminado: `https://s3.amazonaws.com/`

Requerido: No

`--region` region

La región que se usa en la firma de la solicitud.

Valor predeterminado: `us-east-1`

Obligatorio: obligatorio si se usa la versión 4 de firma

`--sigv` version

La versión de la firma que se usará cuando se firme la solicitud.

Valores válidos: 2 | 4

Valor predeterminado: `4`

Requerido: No

`-m, --manifest` file

El nombre del archivo de manifiesto (sin la ruta). Recomendamos que especifique el manifiesto (`-m`) o un prefijo (`-p`).

Requerido: No

`-p, --prefix` prefix

El prefijo de nombre de archivo de los archivos de la AMI agrupados.

Valor predeterminado: `image`

Requerido: No

`-d, --directory` directory

El directorio donde se guarda la agrupación descargada. El directorio debe existir.

Valor predeterminado: el directorio de trabajo actual.

Requerido: No

`--retry`

Reintenta automáticamente en todos los errores de Amazon S3, hasta cinco veces por operación.

Requerido: no

Salida

Se muestran los mensajes de estado que indican las distintas fases del proceso de descarga.

Ejemplo

En este ejemplo se crea el directorio `bundled` (usando el comando de Linux mkdir) y se descarga la agrupación desde el bucket de Amazon S3 `DOC-EXAMPLE-BUCKET1`.

```
[ec2-user ~]$ mkdir bundled
[ec2-user ~]$ ec2-download-bundle -b DOC-EXAMPLE-BUCKET1/bundles/bundle_name
 -m image.manifest.xml -a your_access_key_id -s your_secret_access_key -k pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -d mybundle
```

```
Downloading manifest image.manifest.xml from DOC-EXAMPLE-BUCKET1 to mybundle/
image.manifest.xml ...
Downloading part image.part.00 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to
 mybundle/image.part.00 ...
Downloaded image.part.00 from DOC-EXAMPLE-BUCKET1
Downloading part image.part.01 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to
 mybundle/image.part.01 ...
Downloaded image.part.01 from DOC-EXAMPLE-BUCKET1
Downloading part image.part.02 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to
 mybundle/image.part.02 ...
Downloaded image.part.02 from DOC-EXAMPLE-BUCKET1
Downloading part image.part.03 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to
 mybundle/image.part.03 ...
Downloaded image.part.03 from DOC-EXAMPLE-BUCKET1
Downloading part image.part.04 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to
 mybundle/image.part.04 ...
Downloaded image.part.04 from DOC-EXAMPLE-BUCKET1
Downloading part image.part.05 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to
 mybundle/image.part.05 ...
Downloaded image.part.05 from DOC-EXAMPLE-BUCKET1
Downloading part image.part.06 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to
 mybundle/image.part.06 ...
Downloaded image.part.06 from DOC-EXAMPLE-BUCKET1
```

ec2-migrate-manifest

Descripción

Modifica una AMI de Linux con respaldo en el almacén de instancias (por ejemplo, su certificado, kernel y disco RAM) para que admita una región diferente.

Sintaxis

ec2-migrate-manifest -c *path* -k *path* -m *path* {(-a *access_key_id* -s *secret_access_key* --region *region*) | (--no-mapping)} [--ec2cert *ec2_cert_path*] [--kernel *kernel-id*] [--ramdisk *ramdisk_id*]

Opciones

`-c, --cert` path

El archivo RSA de certificado de clave pública en código PEM del usuario.

Obligatorio: sí

`-k, --privatekey` path

La ruta del archivo de clave RSA en código PEM del usuario.

Obligatorio: sí

`--manifest` path

La ruta del archivo de manifiesto.

Obligatorio: sí

`-a, --access-key` access_key_id

El ID de la clave de acceso de AWS.

Obligatorio: obligatorio si se utiliza el mapeo automático.

`-s, --secret-key` secret_access_key

La clave de acceso secreta de AWS.

Obligatorio: obligatorio si se utiliza el mapeo automático.

`--region` region

La región que se busca en el archivo de mapeo.

Obligatorio: obligatorio si se utiliza el mapeo automático.

`--no-mapping`

Deshabilita el mapeo automático de los kernels y discos RAM.

Durante la migración, Amazon EC2 remplaza el kernel y el disco RAM en el archivo de manifiesto con un kernel y un disco RAM diseñado para la región de destino. Salvo que se proporcione el parámetro `--no-mapping`, `ec2-migrate-bundle` puede usar las operaciones `DescribeRegions` y `DescribeImages` para llevar a cabo mapeos automáticos.

Obligatorio: obligatorio si no proporciona las opciones `-a`, `-s` y `--region` usadas para el mapeo automático.

`--ec2cert` path

La ruta del certificado de clave pública Amazon EC2 X.509 utilizado para cifrar el manifiesto de la imagen.

Las regiones `us-gov-west-1` y `cn-north-1` usan un certificado de clave pública no predeterminado y la ruta de dicho certificado debe especificarse con esta opción. La ruta del certificado varía según el método de instalación de las herramientas para AMI. En Amazon Linux, los certificados se encuentran en `/opt/aws/amitools/ec2/etc/ec2/amitools/`. Si ha instalado las herramientas para AMI del archivo ZIP en Configurar las herramientas de la AMI, los certificados se encuentran en `$EC2_AMITOOL_HOME/etc/ec2/amitools/`.

Obligatorio: solo para las regiones `us-gov-west-1` y `cn-north-1`.

`--kernel` kernel_id

El ID del kernel que se va seleccionar.

> **Important**
>
> Recomendamos que use PV-GRUB en lugar de kernels y discos RAM. Para obtener más información, consulte User provided kernels en la Guía del usuario de Amazon Linux 2.

Requerido: no

`--ramdisk` ramdisk_id

El ID del disco RAM para seleccionar.

> **Important**
>
> Recomendamos que use PV-GRUB en lugar de kernels y discos RAM. Para obtener más información, consulte User provided kernels en la Guía del usuario de Amazon Linux 2.

Requerido: no

Salida

Mensajes de estado que describen las fases y los estados del proceso de agrupación.

Ejemplo

En este ejemplo se copia la AMI especificada en el manifiesto `my-ami.manifest.xml` de EE. UU. en la UE.

```
[ec2-user ~]$ ec2-migrate-manifest --manifest my-ami.manifest.xml
 --cert cert-HKZYKTAIG2ECMXYIBH3HXV4ZBZQ55CLO.pem --privatekey pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBZQ55CLO.pem --region eu-west-1

Backing up manifest...
Successfully migrated my-ami.manifest.xml It is now suitable for use in eu-west-1.
```

ec2-unbundle

Descripción

Crea de nuevo la agrupación desde una AMI de Linux con respaldo en el almacén de instancias.

Sintaxis

ec2-unbundle -k *path* -m *path* [-s *source_directory*] [-d *destination_directory*]

Opciones

`-k, --privatekey` path

La ruta del archivo de clave RSA en código PEM.

Obligatorio: sí

`-m, --manifest` path

La ruta del archivo de manifiesto.

Obligatorio: sí

`-s, --source` source_directory

El directorio que contiene la agrupación.

Valor predeterminado: el directorio actual.

Requerido: No

`-d, --destination` destination_directory

El directorio donde se desagrupa la AMI. El directorio de destino debe existir.

Valor predeterminado: el directorio actual.

Requerido: no

Ejemplo

En este ejemplo de Linux y UNIX se desagrupa la AMI especificada en el archivo `image.manifest.xml`.

```
[ec2-user ~]$ mkdir unbundled
$ ec2-unbundle -m mybundle/image.manifest.xml -k pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -s mybundle -d unbundled
$ ls -l unbundled
total 1025008
-rw-r--r-- 1 root root 1048578048 Aug 25 23:46 image.img
```

Salida

Se muestran los mensajes de estado que indican las distintas fases del proceso de desagrupación.

ec2-upload-bundle

Descripción

Carga el paquete de una AMI de Linux respaldada por el almacén de instancias en Amazon S3 y establece las listas de control de acceso (ACL) adecuadas en los objetos cargados. Para obtener más información, consulte Crear una AMI de Linux con respaldo en el almacén de instancias.

> **Note**
>
> Para cargar objetos en un bucket de S3 para la AMI de Linux respaldada por el almacén de instancias, las ACL deben estar habilitadas para el bucket. De lo contrario, Amazon EC2 no podrá configurar las ACL en los objetos que se van a cargar. Si el bucket de destino utiliza la configuración impuesta por el propietario del bucket para la propiedad de objetos de S3, esto no funcionará porque las ACL están deshabilitadas. Para obtener más información, consulte Control de la propiedad de objetos cargados mediante la propiedad de objetos de S3.

Sintaxis

```
ec2-upload-bundle -b bucket -a access_key_id -s secret_access_key [-t
token] -m path [--url url] [--region region] [--sigv version] [--acl acl]
[-d directory] [--part part] [--retry] [--skipmanifest]
```

Opciones

`-b, --bucket` bucket

El nombre del bucket de Amazon S3 donde se almacena la agrupación, seguido de un prefijo de ruta delimitado por '/' opcional. Si el bucket no existe, se crea si se dispone del nombre del bucket. Además, si el bucket no existe y la versión de las herramientas de AMI es la 1.5.18 o posterior, este comando establece las ACL del bucket.

Obligatorio: sí

`-a, --access-key` access_key_id

El ID de la clave de acceso de AWS.

Obligatorio: sí

`-s, --secret-key` secret_access_key

La clave de acceso secreta de AWS.

Obligatorio: sí

`-t, --delegation-token` token

El token de delegación que se pasa junto con la solicitud de AWS. Para obtener más información, consulte Uso de credenciales de seguridad temporales.

Obligatorio: solo cuando se utilizan credenciales de seguridad temporales.

Valor predeterminado: el valor de la variable de entorno `AWS_DELEGATION_TOKEN` (si se ha establecido).

`-m, --manifest` path

La ruta del archivo de manifiesto. El archivo de manifiesto se crea durante el proceso de agrupación y se puede encontrar en el directorio que contiene la agrupación.

Obligatorio: sí

`--url` url

Obsoleto. Use la opción `--region` en su lugar salvo que el bucket esté restringido a la ubicación `EU` (y no `eu-west-1`). La marca `--location` es el único modo de controlar esa limitación de ubicación específica.

La URL de servicio del punto de conexión de Amazon S3

Valor predeterminado: `https://s3.amazonaws.com/`

Requerido: No

`--region` region

La región que se va a usar en la firma de la solicitud del bucket de destino de S3.

- Si el bucket no existe y no especifica una región, la herramienta crea el bucket sin una limitación de ubicación (en `us-east-1`).
- Si el bucket no existe y especifica una región, la herramienta crea el bucket en la región especificada.
- Si el bucket existe y no especifica una región, la herramienta usa la ubicación del bucket.
- Si el bucket existe y especifica `us-east-1` como región, la herramienta usa la ubicación del bucket sin ningún mensaje de error y cualquier archivo existente que coincida se sobrescribe.
- Si el bucket existe y especifica una región (distinta de `us-east-1`) que no coincida con la ubicación real del bucket, la herramienta sale sin dar error.

Si el bucket esté restringido a la ubicación EU (y no `eu-west-1`), use la marca `--location` en su lugar. La marca `--location` es el único modo de controlar esa limitación de ubicación específica.

Valor predeterminado: `us-east-1`

Obligatorio: obligatorio si se usa la versión 4 de firma

`--sigv` version

La versión de la firma que se usará cuando se firme la solicitud.

Valores válidos: `2` | `4`

Valor predeterminado: `4`

Requerido: No

`--acl` acl

La política de la lista de control de acceso de la imagen agrupada.

Valores válidos: `public-read` | `aws-exec-read`

Valor predeterminado: `aws-exec-read`

Requerido: No

`-d, --directory` directory

El directorio que contiene las partes de AMI agrupadas.

Valor predeterminado: el directorio que contiene el archivo de manifiesto (consulte la opción `-m`).

Requerido: No

`--part` part

Comienza a cargar la parte especificada y todas las partes subsecuentes. Por ejemplo, `--part 04`.

Requerido: No

`--retry`

Reintenta automáticamente en todos los errores de Amazon S3, hasta cinco veces por operación.

Requerido: No

`--skipmanifest`

No carga el manifiesto.

Requerido: No

`--location` location

Obsoleto. Use la opción `--region` en su lugar, salvo que el bucket esté restringido a la ubicación EU (y no `eu-west-1`). La marca `--location` es el único modo de controlar esa limitación de ubicación específica.

La restricción de ubicación del bucket de Amazon S3 de destino. Si el bucket existe y especifica una ubicación que no coincide con la ubicación real del bucket, la herramienta sale sin dar error. Si el bucket existe y no especifica una ubicación, la herramienta usa la ubicación del bucket. Si el bucket no existe y especifica una ubicación, la herramienta crea el bucket en la ubicación especificada. Si el bucket no existe y no especifica una ubicación, la herramienta crea el bucket sin una restricción de ubicación (en `us-east-1`).

Valor predeterminado: si se especifica `--region`, la ubicación se establece en esa región especificada. Si no se especifica `--region`, la ubicación predeterminada es `us-east-1`.

Requerido: no

Salida

Amazon EC2 muestra mensajes de estado que indican las fases y el estado del proceso de carga.

Ejemplo

En este ejemplo se carga la agrupación especificada en el manifiesto `image.manifest.xml`.

```
[ec2-user ~]$ ec2-upload-bundle -b DOC-EXAMPLE-BUCKET1/bundles/bundle_name -m
 image.manifest.xml -a your_access_key_id -s your_secret_access_key
Creating bucket...
Uploading bundled image parts to the S3 bucket DOC-EXAMPLE-BUCKET1 ...
Uploaded image.part.00
Uploaded image.part.01
Uploaded image.part.02
Uploaded image.part.03
Uploaded image.part.04
Uploaded image.part.05
Uploaded image.part.06
Uploaded image.part.07
Uploaded image.part.08
Uploaded image.part.09
Uploaded image.part.10
Uploaded image.part.11
Uploaded image.part.12
Uploaded image.part.13
Uploaded image.part.14
Uploading manifest ...
Uploaded manifest.
Bundle upload completed.
```

Opciones comunes de las herramientas para AMI

La mayoría de las herramientas para AMI aceptan los siguientes parámetros opcionales.

`--help, -h`

Muestra el mensaje de ayuda.

`--version`

Muestra la versión y el aviso de copyright.

`--manual`

Muestra la entrada manual.

`--batch`

Se ejecuta en modo por lotes y se suspenden las preguntas interactivas.

`--debug`

Muestra información que puede ser útil para la solución de problemas.

Creación de una AMI con Windows Sysprep

La herramienta Microsoft System Preparation (Sysprep) simplifica el proceso de duplicado de una instalación personalizada de Windows. Puede utilizar Sysprep para crear una Imagen de máquina de Amazon (AMI) estandarizada. Luego, cree instancias de Amazon EC2 para Windows a partir de esta imagen estandarizada.

Recomendamos que utilice EC2 Image Builder para automatizar la creación, administración e implementación de imágenes de servidor “doradas” personalizadas, seguras y actualizadas que estén preinstaladas y preconfiguradas con software y configuración.

Si utiliza Windows Sysprep para crear una AMI estandarizada, se recomienda que ejecute Sysprep con EC2Launch v2. Si aún utiliza los agentes EC2Config (Windows Server 2012 R2 y anteriores) o EC2Launch (Windows Server 2016 y 2019), consulte la documentación sobre el uso de Sysprep con EC2Config y EC2Launch que se muestra a continuación.

> **Important**
>
> No utilice Sysprep para crear una copia de seguridad de instancias. Sysprep elimina información específica del sistema; la eliminación de dicha información podría tener consecuencias no deseadas para el backup de instancias.

Para solucionar problemas de Sysprep, consulte Solución de problemas de Sysprep con instancias de Windows.

Contenido

Antes de empezar

- Antes de ejecutar Sysprep, se recomienda que elimine todas las cuentas de usuarios locales y todos los perfiles de cuentas distintos de las cuentas de un único administrador en las que se ejecutará Sysprep. Si ejecuta Sysprep con otras cuentas y perfiles, es posible que se produzca un comportamiento inesperado, incluida la pérdida de datos de perfiles o la imposibilidad de completar Sysprep.
- Encontrará más información sobre Sysprep en Microsoft TechNet.
- Descubra qué roles de servidor admite Sysprep.

Uso de Sysprep con EC2Launch v2

Esta sección contiene detalles sobre las diferentes fases de ejecución de Sysprep y las tareas realizadas por el servicio de EC2Launch v2 a medida que se prepara la imagen. También incluye los pasos para crear una AMI estandarizada usando Sysprep con el servicio de EC2Launch v2.

Sysprep con temas de EC2Launch v2

Fases de Sysprep

Sysprep se ejecuta en las siguientes fases:

- Generalize: la herramienta elimina la información y la configuración específicas de la imagen. Por ejemplo, Sysprep elimina el identificador de seguridad (SID), el nombre del equipo, los registros de eventos y los controladores específicos, por citar solo algunos. Una vez completada esta fase, el sistema operativo (OS) está listo para crear una AMI.

> **Note**
>
> Cuando ejecuta Sysprep con el servicio de EC2Launch v2, el sistema evita que se quiten los controladores porque la configuración `PersistAllDeviceInstalls` está establecida en true de forma predeterminada.

- Specialize: La configuración "Plug and Play" analiza el equipo e instala controladores para cualquier dispositivo detectado. La herramienta genera los requisitos del sistema operativo, como el nombre del equipo y el SID. Opcionalmente, puede ejecutar comandos en esta fase.
- Out-of-Box Experience (OOBE): el sistema ejecuta una versión abreviada de Windows Setup y le solicita que escriba información como el idioma del sistema, la zona horaria y una organización registrada. Al ejecutar Sysprep con EC2Launch v2, el archivo de respuestas automatiza esta fase.

Acciones de Sysprep

Sysprep y EC2Launch v2 realizan las siguientes acciones al preparar una imagen.

1. Cuando elige Shutdown with Sysprep en el cuadro de diálogo de EC2Launch settings, el sistema ejecuta el comando `ec2launch sysprep`.
2. EC2Launch v2 edita el contenido del archivo `unattend.xml` leyendo el valor del registro en `HKEY_USERS\.DEFAULT\Control Panel\International\LocaleName`. El archivo se encuentra en el siguiente directorio: `C:\ProgramData\Amazon\EC2Launch\sysprep`.
3. El sistema ejecuta `BeforeSysprep.cmd`. Este comando crea una clave del Registro como la siguiente:

   reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 1 /f

   La clave de registro deshabilita las conexiones RDP hasta que se vuelvan a habilitar. Deshabilitar las conexiones RDP es una medida de seguridad necesaria porque, durante la primera sesión de arranque tras ejecutarse Sysprep, hay un breve período de tiempo en el que RDP permite las conexiones y la contraseña del administrador está vacía.
4. El servicio EC2Launch v2 llama a Sysprep mediante la ejecución del siguiente comando:

   sysprep.exe /oobe /generalize /shutdown /unattend: "C:\ProgramData\Amazon\EC2Launch \sysprep\unattend.xml"

Fase Generalize

- EC2Launch v2 elimina la información y la configuración específicas de la imagen, como el nombre del equipo y el SID. Si la instancia pertenece a un dominio, se elimina de dicho dominio. El archivo de respuestas `unattend.xml` incluye la siguiente configuración que afecta a esta fase:
  - PersistAllDeviceInstalls: Esta configuración evita que Windows Setup elimine y vuelva a configurar dispositivos, lo que acelera el proceso de preparación de imágenes, ya que las AMI de Amazon requieren la ejecución de ciertos controladores y la nueva detección de dichos controladores podría llevar tiempo.
  - DoNotCleanUpNonPresentDevices: Esta configuración conserva la información Plug and Play de los dispositivos que no están presentes en ese momento.
- Sysprep apaga el sistema operativo al prepararse para crear la AMI. El sistema inicia una nueva instancia o bien inicia la instancia original.

Fase Specialize

El sistema genera los requisitos específicos del sistema operativo, como el nombre del equipo y un SID. Además, el sistema realiza las siguientes acciones en función de la configuración que especifique en el archivo de respuestas `unattend.xml`.

- CopyProfile: Sysprep se puede configurar para eliminar todos los perfiles de usuario, incluido el perfil de administrador integrado. Esta configuración conserva la cuenta de administrador incorporada para que cualquier personalización que realice en la cuenta se traslade a la nueva imagen. El valor predeterminado es `True`.

  CopyProfile sustituye el perfil predeterminado con el perfil de administrador local existente. Todas las cuentas en las que inicie sesión después de ejecutar Sysprep recibirán una copia de dicho perfil y su contenido en el primer inicio de sesión.

  Si no tiene ninguna personalización de perfiles de usuario específica que desee trasladar a la nueva imagen, cambie esta configuración a `False`. Sysprep eliminará todos los perfiles de usuario (esto permite ahorrar tiempo y espacio en disco.
- TimeZone: de forma predeterminada, la zona horaria está establecida en tiempo universal coordinado (UTC).
- Synchronous command with order 1: El sistema ejecuta el siguiente comando que habilita la cuenta de administrador y especifica el requisito de contraseña:

```
net user Administrator /ACTIVE:YES /LOGONPASSWORDCHG:NO /EXPIRES:NEVER /
PASSWORDREQ:YES
```

- Synchronous command with order 2: El sistema codifica la contraseña de administrador. Esta medida de seguridad está diseñada para evitar que se pueda acceder a la instancia después de que Sysprep se complete si no habilitó la configuración de la tarea `setAdminAccount`.

  El sistema ejecuta el siguiente comando desde el directorio local de agentes de lanzamiento (`C:\Program Files\Amazon\EC2Launch\`).

  ```
  EC2Launch.exe internal randomize-password --username Administrator
  ```

- Para habilitar las conexiones de escritorio remoto, el sistema establece la clave de registro de Terminal Server `fDenyTSConnections` en falso.

Fase OOBE

1. El sistema especifica las siguientes configuraciones mediante el archivo de respuesta de EC2Launch v2:
   - `<InputLocale>en-US</InputLocale>`
   - `<SystemLocale>en-US</SystemLocale>`
   - `<UILanguage>en-US</UILanguage>`
   - `<UserLocale>en-US</UserLocale>`
   - `<HideEULAPage>true</HideEULAPage>`
   - `<HideWirelessSetupInOOBE>true</HideWirelessSetupInOOBE>`
   - `<ProtectYourPC>3</ProtectYourPC>`
   - `<BluetoothTaskbarIconEnabled>false</BluetoothTaskbarIconEnabled>`
   - `<TimeZone>UTC</TimeZone>`
   - `<RegisteredOrganization>Amazon.com</RegisteredOrganization>`
   - `<RegisteredOwner>EC2</RegisteredOwner>`

> **Note**
>
> Durante las fases de generalización y especialización, EC2Launch v2 monitorea el estado del sistema operativo. Si EC2Launch v2 detecta que el sistema operativo se encuentra en una fase de Sysprep, publica el siguiente mensaje en el registro del sistema:
> Se está configurando Windows. SysprepState=IMAGE_STATE_UNDEPLOYABLE

2. El sistema ejecuta EC2Launch v2.

Después de Sysprep

Después de que Sysprep se complete, EC2Launch v2 envía el siguiente mensaje a la salida de la consola:

```
Windows sysprep configuration complete.
```

A continuación, EC2Launch v2 realiza las siguientes acciones:

1. Lee el contenido del archivo `agent-config.yml` y ejecuta las tareas configuradas.
2. Ejecuta todas las tareas de la etapa `preReady`.
3. Después de que finalice, envía un mensaje `Windows is ready` a los registros del sistema de la instancia.
4. Ejecuta todas las tareas de la etapa `PostReady`.

Para obtener más información acerca de EC2Launch v2, consulte Configurar una instancia de Windows mediante EC2Launch v2.

Ejecutar Sysprep con EC2Launch v2

Utilice el procedimiento siguiente para crear una AMI estandarizada mediante Sysprep con EC2Launch v2.

1. En la consola de Amazon EC2, localice una AMI que desee duplicar.
2. Lance y conéctese a la instancia de Windows.
3. Personalícela.

4. En el menú de Inicio de Windows, busque y elija Configuración de Amazon EC2Launch. Para obtener más información sobre las opciones y la configuración del cuadro de diálogo Configuración de EC2Launch de Amazon, consulte Configuración de EC2Launch v2.
5. Seleccione Cerrar con Sysprep o Cerrar sin Sysprep.

Cuando se le solicite que confirme que desea ejecutar Sysprep y cerrar la instancia, haga clic en Yes. EC2Launch v2 ejecuta Sysprep. A continuación, se cierra la sesión en la instancia y esta se cierra. Si comprueba la página Instancias en la consola de Amazon EC2, el estado de la instancia cambia de `Running` a `Stopping` a `Stopped`. En este momento, es seguro crear una AMI desde esta instancia.

Puede invocar la herramienta Sysprep manualmente desde la línea de comando utilizando el siguiente comando:

```
"%programfiles%\amazon\ec2launch\ec2launch.exe" sysprep --shutdown=true
```

Uso de Sysprep con EC2Launch

EC2Launch ofrece un archivo de respuestas predeterminado y archivos de lotes para Sysprep que automatizan y protegen el proceso de preparación de imágenes de la AMI. Es opcional modificar estos archivos. Estos archivos se encuentran de manera predeterminada en el siguiente directorio: `C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep`.

> **Important**
>
> No utilice Sysprep para crear una copia de seguridad de instancias. Sysprep elimina la información específica del sistema. Si elimina esta información, podrían producirse consecuencias no deseadas en una copia de seguridad de instancias.

Sysprep con temas de EC2Launch

- Archivos por lotes y respuestas de EC2Launch para Sysprep
- Ejecute Sysprep con EC2Launch.
- Actualice las rutas de metadatos/KMS para Server 2016 y versiones posteriores al iniciar una AMI personalizada.

Archivos por lotes y respuestas de EC2Launch para Sysprep

El archivo de respuestas EC2Launch y los archivos de lotes de Sysprep incluyen lo siguiente:

`Unattend.xml`

Este es el archivo de respuestas predeterminado. Si ejecuta `SysprepInstance.ps1` o elige ShutdownWithSysprep en la interfaz de usuario, el sistema lee los ajustes en este archivo.

`BeforeSysprep.cmd`

Personalice este archivo de lote para que ejecute comandos antes de que EC2Launch ejecute Sysprep.

`SysprepSpecialize.cmd`

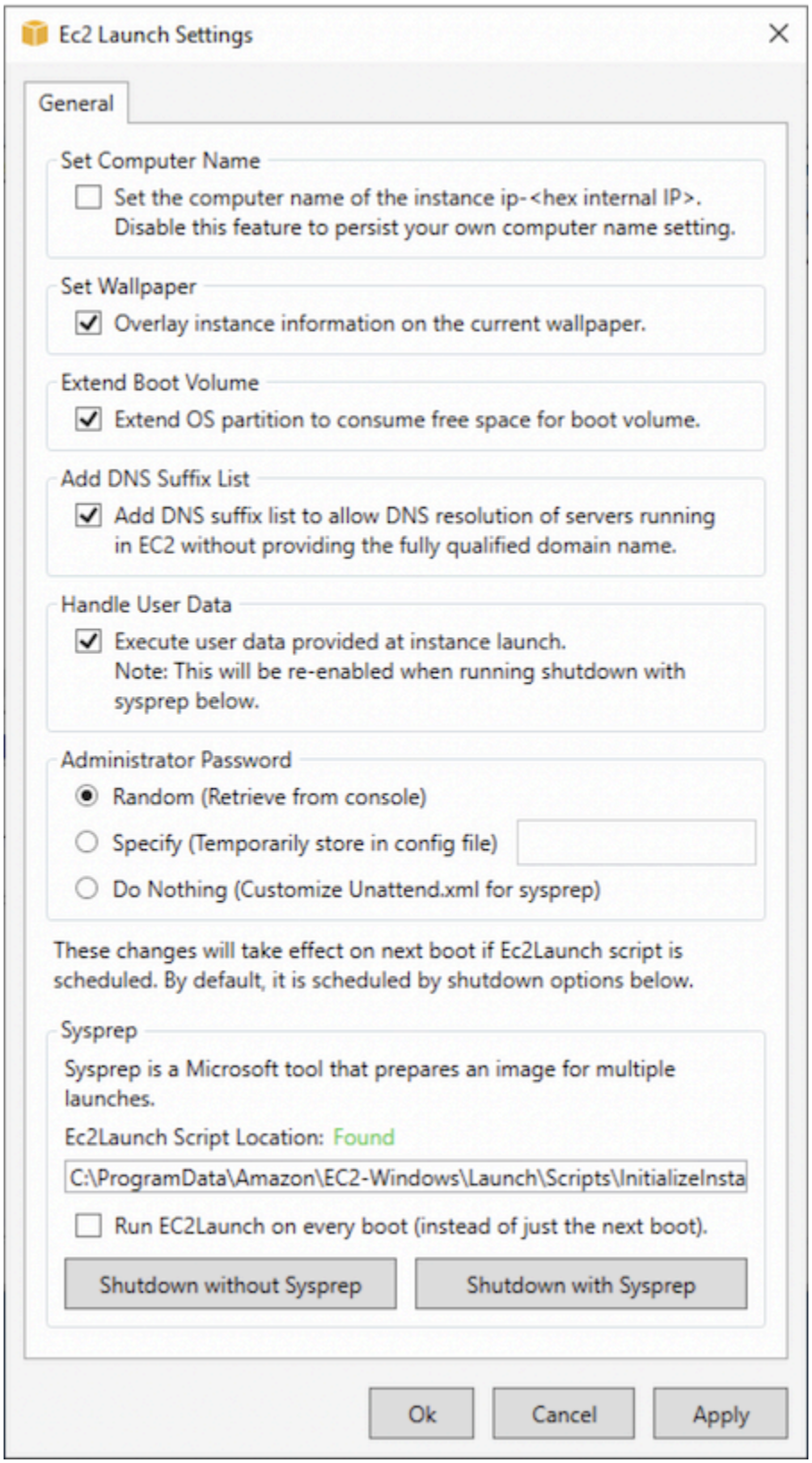
Personalice este archivo de lote para que ejecute comandos durante la fase de especialización de Sysprep.

Ejecute Sysprep con EC2Launch.

En la instalación completa de Windows Server 2016 y versiones posteriores (con la experiencia de escritorio), puede ejecutar Sysprep con EC2Launch manualmente o con la aplicación EC2 Launch Settings.

Para ejecutar Sysprep utilizando la aplicación EC2Launch Settings

1. En la consola de Amazon EC2, localice o cree una AMI de Windows Server 2016 o posterior.
2. Lance una instancia de Windows desde la AMI.
3. Conéctese a la instancia de Windows y personalícela.
4. Busque la aplicación EC2LaunchSettings y ejecútela. De forma predeterminada, se encuentra en el siguiente directorio: `C:\ProgramData\Amazon\EC2-Windows\Launch\Settings`.



5. Seleccione o borre las opciones que correspondan. Esta configuración se almacena en el archivo `LaunchConfig.json`.

6. En Contraseña del administrador, realice una de las acciones siguientes:

   - Elija Asignación al azar. EC2Launch genera una contraseña y la cifra usando la clave del usuario. El sistema deshabilita esta configuración tras la inicialización de la instancia para que esta contraseña persista si la instancia se reinicia o si se detiene y se inicia.
   - Elija Especificarla y escriba una contraseña que cumpla los requisitos del sistema. La contraseña se almacena en `LaunchConfig.json` como texto sin cifrar y se elimina cuando Sysprep define la contraseña del administrador. Si apaga en equipo en este momento, la contraseña se establece inmediatamente. EC2Launch cifra la contraseña usando la clave del usuario.
   - Elija No hacer nada y especifique una contraseña en el archivo `unattend.xml`. Si no especifica una contraseña en el archivo `unattend.xml`, la cuenta del administrador se deshabilitará.

7. Elija Cerrar con Sysprep.

Para ejecutar Sysprep manualmente utilizando EC2Launch

1. En la consola de Amazon EC2, localice o cree una AMI para Windows Server 2016 Datacenter Edition o posterior que desee duplicar.
2. Lance y conéctese a la instancia de Windows.
3. Personalice la instancia.
4. Especifique las opciones en el archivo `LaunchConfig.json`. De forma predeterminada, este archivo se encuentra en el directorio `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.

   En `adminPasswordType`, especifique uno de los siguientes valores:

   `Random`

   EC2Launch genera una contraseña y la cifra usando la clave del usuario. El sistema deshabilita esta configuración tras la inicialización de la instancia para que esta contraseña persista si la instancia se reinicia o si se detiene y se inicia.

   `Specify`

   EC2Launch usa la contraseña que ha especificado en `adminPassword`. Si la contraseña no cumple los requisitos del sistema, EC2Launch genera una contraseña aleatoria en su lugar. La contraseña se almacena en `LaunchConfig.json` como texto sin cifrar y se elimina

cuando Sysprep define la contraseña del administrador. EC2Launch cifra la contraseña usando la clave del usuario.

`DoNothing`

EC2Launch usa la contraseña que ha especificado en el archivo `unattend.xml`. Si no especifica una contraseña en el archivo `unattend.xml`, la cuenta del administrador se deshabilitará.

5. (Opcional) Especifique los ajustes en `unattend.xml` y en los otros archivos de configuración. Si tiene pensado estar presente durante la instalación, no es necesario que realice cambios en estos archivos. Los archivos se encuentran de manera predeterminada en el siguiente directorio: `C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep`.
6. En Windows PowerShell, ejecute `./InitializeInstance.ps1 -Schedule`. De forma predeterminada, el script se encuentra en el siguiente directorio: `C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts`. Este script programa la instancia para que se inicialice durante el siguiente arranque. Debe ejecutar este script antes de ejecutar el script `SysprepInstance.ps1` en el paso siguiente.
7. En Windows PowerShell, ejecute `./SysprepInstance.ps1`. De forma predeterminada, el script se encuentra en el siguiente directorio: `C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts`.

Se cierra la sesión en la instancia y esta se cierra. Si comprueba la página Instancias en la consola de Amazon EC2, el estado de la instancia cambia de `Running` a `Stopping` y, a continuación, a `Stopped`. En este punto es seguro crear una AMI desde esta instancia.

Actualice las rutas de metadatos/KMS para Server 2016 y versiones posteriores al iniciar una AMI personalizada.

Para actualizar las rutas de metadatos/KMS para Server 2016 y versiones posteriores al iniciar una AMI personalizada, aplique alguna de las siguientes acciones:

- Ejecute la GUI EC2LaunchSettings (C:\ProgramData\Amazon\EC2-Windows\Launch\Settings\Ec2LaunchSettings.exe) y seleccione la opción para cerrar el sistema con Sysprep.
- Ejecute EC2LaunchSettings y cierre el sistema sin Sysprep antes de crear la AMI. Esto establece las tareas de inicialización de inicialización de EC2 para que se ejecuten en el siguiente arranque; con ello, se establecen las rutas basadas en la subred para la instancia.

- Si lo prefiere, puede reprogramar manualmente las tareas de inicialización de inicialización de EC2 antes de crear una AMI desde PowerShell.

> **Important**
>
> Tenga en cuenta el comportamiento predeterminado de restablecimiento de contraseña antes de reprogramar las tareas.

- Para actualizar las rutas en una instancia en ejecución en la que se produzcan errores en sus metadatos durante la activación o comunicación con Windows, consulte "No se puede activar Windows".

Uso de Sysprep con EC2Config

Esta sección contiene detalles sobre las diferentes fases de ejecución de Sysprep y las tareas realizadas por el servicio de EC2Config a medida que se prepara la imagen. También incluye los pasos para crear una AMI estandarizada utilizando Sysprep con el servicio EC2Config.

Sysprep con temas de EC2Config

- Fases de Sysprep
- Acciones de Sysprep
- Después de Sysprep
- Ejecución de Sysprep con el servicio EC2Config

Fases de Sysprep

Sysprep se ejecuta en las siguientes fases:

- Generalize: la herramienta elimina la información y la configuración específicas de la imagen. Por ejemplo, Sysprep elimina el identificador de seguridad (SID), el nombre del equipo, los registros de eventos y los controladores específicos, por citar solo algunos. Una vez completada esta fase, el sistema operativo (OS) está listo para crear una AMI.

> **Note**
>
> Al ejecutar Sysprep con el servicio EC2Config, el sistema evita que se eliminen los controladores porque la configuración de PersistAllDeviceInstalls está establecida como true de forma predeterminada.

- Specialize: La configuración "Plug and Play" analiza el equipo e instala controladores para cualquier dispositivo detectado. La herramienta genera los requisitos del sistema operativo, como el nombre del equipo o el SID. Opcionalmente, puede ejecutar comandos en esta fase.
- Out-of-Box Experience (OOBE): el sistema ejecuta una versión abreviada de Windows Setup y solicita al usuario que escriba información como el idioma del sistema, la zona horaria o una organización registrada. Al ejecutar Sysprep con EC2Config, el archivo de respuestas automatiza esta fase.

Acciones de Sysprep

Sysprep y el servicio EC2Config realizan las siguientes acciones al preparar una imagen.

1. Cuando elige Apagado con Sysprep en el cuadro de diálogo Propiedades del servicio EC2, el sistema ejecuta el comando ec2config.exe -sysprep.
2. El servicio EC2Config lee el contenido del archivo `BundleConfig.xml`. De forma predeterminada, este archivo está ubicado en el siguiente directorio: `C:\Program Files\Amazon\Ec2ConfigService\Settings`.

   El archivo `BundleConfig.xml` incluye la siguiente configuración. Puede cambiar esta configuración:

   - AutoSysprep: Indica si utilizar Sysprep automáticamente. No es necesario cambiar este valor si ejecuta Sysprep desde el cuadro de diálogo EC2 Service Properties. El valor predeterminado es `No`.
   - SetRDPCertificate: establece un certificado autofirmado para el servidor de Escritorio remoto. De este modo puede utilizar el Protocolo de escritorio remoto (RDP) de forma segura para conectarse a la instancia. Si las nuevas instancias deben utilizar un certificado, cambie el valor a `Yes`. Esta configuración no se utiliza con instancias de Windows Server 2012 porque estos sistemas operativos pueden generar sus propios certificados. El valor predeterminado es `No`.
   - SetPasswordAfterSysprep: establece una contraseña aleatoria para una instancia recién iniciada, la cifra con la clave de inicialización del usuario y devuelve la contraseña cifrada a la

consola. Si las nuevas instancias no deben configurarse con una contraseña cifrada aleatoria, cambie el valor a `No`. El valor predeterminado es `Yes`.

- PreSysprepRunCmd: La ubicación del comando que se debe ejecutar. De forma predeterminada, el comando se encuentra en el siguiente directorio: `C:\Program Files\Amazon\Ec2ConfigService\Scripts\BeforeSysprep.cmd`

3. El sistema ejecuta `BeforeSysprep.cmd`. Este comando crea una clave del Registro como la siguiente:

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v
 fDenyTSConnections /t REG_DWORD /d 1 /f
```

   La clave de registro deshabilita las conexiones RDP hasta que se vuelvan a habilitar. Deshabilitar las conexiones RDP es una medida de seguridad necesaria porque, durante la primera sesión de arranque tras ejecutarse Sysprep, hay un breve período de tiempo en el que RDP permite las conexiones y la contraseña del administrador está vacía.

4. El servicio EC2Config llama a Sysprep ejecutando el siguiente comando:

```
sysprep.exe /unattend: "C:\Program Files\Amazon\Ec2ConfigService\sysprep2008.xml" /
oobe /generalize /shutdown
```

Fase Generalize

- La herramienta elimina la información y la configuración específicas de la imagen, como el nombre del equipo y el SID. Si la instancia pertenece a un dominio, se elimina de dicho dominio. El archivo de respuestas `sysprep2008.xml` incluye la siguiente configuración que afecta a esta fase:
  - PersistAllDeviceInstalls: Esta configuración evita que Windows Setup elimine y vuelva a configurar dispositivos, lo que acelera el proceso de preparación de imágenes, ya que las AMI de Amazon requieren la ejecución de ciertos controladores y la nueva detección de dichos controladores podría llevar tiempo.
  - DoNotCleanUpNonPresentDevices: Esta configuración conserva la información Plug and Play de los dispositivos que no están presentes en ese momento.
- Sysprep apaga el sistema operativo al prepararse para crear la AMI. El sistema inicia una nueva instancia o bien inicia la instancia original.

Fase Specialize

El sistema genera los requisitos específicos del sistema operativo, como el nombre del equipo o un SID. Además, el sistema realiza las siguientes acciones, en función de la configuración que especifique en el archivo de respuestas sysprep2008.xml.

- CopyProfile: Sysprep se puede configurar para eliminar todos los perfiles de usuario, incluido el perfil de administrador integrado. Esta configuración conserva la cuenta de administrador incorporada para que cualquier personalización que haya realizado en la cuenta se traslade a la nueva imagen. El valor predeterminado es True.

  CopyProfile sustituye el perfil predeterminado con el perfil de administrador local existente. Todas las cuentas en las que se haya iniciado sesión después de ejecutar Sysprep recibirán una copia de dicho perfil y su contenido en el primer inicio de sesión.

  Si no tiene ninguna personalización de perfiles de usuario específica que desee trasladar a la nueva imagen, cambie esta configuración a False. Sysprep eliminará todos los perfiles de usuario, lo que permite ahorrar tiempo y espacio en disco.
- TimeZone: De forma predeterminada, la zona horaria está establecida en tiempo universal coordinado (UTC).
- Synchronous command with order 1: El sistema ejecuta el siguiente comando que habilita la cuenta de administrador y especifica el requisito de contraseña.

  net user Administrator /ACTIVE:YES /LOGONPASSWORDCHG:NO /EXPIRES:NEVER / PASSWORDREQ:YES
- Synchronous command with order 2: El sistema codifica la contraseña de administrador. Esta medida de seguridad está diseñada para evitar que la instancia se accesible una vez se complete Sysprep si no habilitó la configuración de ec2setpassword.

  C:\Program Files\Amazon\Ec2ConfigService\ScramblePassword.exe" -u Administrator
- Synchronous command with order 3: El sistema ejecuta el siguiente comando:

  C:\Program Files\Amazon\Ec2ConfigService\Scripts\SysprepSpecializePhase.cmd

  Este comando añade la siguiente clave de registro, que vuelve a habilitar RDP:

  añadir reg. "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f

Fase OOBE

1. Utilizando el archivo de respuestas del servicio EC2Config, el sistema especifica las siguientes configuraciones:
   - <InputLocale>en-US</InputLocale>
   - <SystemLocale>en-US</SystemLocale>
   - <UILanguage>en-US</UILanguage>
   - <UserLocale>en-US</UserLocale>
   - <HideEULAPage>true</HideEULAPage>
   - <HideWirelessSetupInOOBE>true</HideWirelessSetupInOOBE>
   - <NetworkLocation>Other</NetworkLocation>
   - <ProtectYourPC>3</ProtectYourPC>
   - <BluetoothTaskbarIconEnabled>false</BluetoothTaskbarIconEnabled>
   - <TimeZone>UTC</TimeZone>
   - <RegisteredOrganization>Amazon.com</RegisteredOrganization>
   - <RegisteredOwner>Amazon</RegisteredOwner>

   > **Note**
   >
   > Durante las fases generalize y specialize, el servicio EC2Config monitoriza el estado del sistema operativo. Si EC2Config detecta que el sistema operativo se encuentra en una fase de Sysprep, publica el siguiente mensaje en el registro del sistema: EC2ConfigMonitorState: 0 Windows is being configured. SysprepState=IMAGE_STATE_UNDEPLOYABLE

2. Una vez completada la fase OOBE, el sistema ejecuta `SetupComplete.cmd` desde la siguiente ubicación: `C:\Windows\Setup\Scripts\SetupComplete.cmd`. En las AMI públicas de Amazon anteriores a abril de 2015, este archivo estaba vacío y no se ejecutaba nada en la imagen. En las AMI públicas con fecha posterior a abril de 2015, el archivo incluye el siguiente valor: call "C:\Program Files\Amazon\Ec2ConfigService\Scripts\PostSysprep.cmd".
3. El sistema ejecuta `PostSysprep.cmd`, que realiza las siguientes operaciones:
   - Establece la contraseña del administrador local de forma que no venza. Si la contraseña vence, es posible que los administradores no puedan iniciar sesión.

- Establece el nombre del equipo de MSSQLServer (si está instalado) para que esté in sincronizado con la AMI.

Después de Sysprep

Una vez se complete Sysprep, el servicio EC2Config envía en siguiente mensaje a la salida de la consola:

```
Windows sysprep configuration complete.
   Message: Sysprep Start
   Message: Sysprep End
```

A continuación, EC2Config realiza las siguientes acciones:

1. Lee el contenido del archivo config.xml y muestra todos los complementos habilitados.
2. Ejecuta todos los complementos “Before Windows is ready” simultáneamente.
   - Ec2SetPassword
   - Ec2SetComputerName
   - Ec2InitializeDrives
   - Ec2EventLog
   - Ec2ConfigureRDP
   - Ec2OutputRDPCert
   - Ec2SetDriveLetter
   - Ec2WindowsActivate
   - Ec2DynamicBootVolumeSize
3. Una vez que ha finalizado, envía el mensaje “Windows is ready” a los registros del sistema de la instancia.
4. Ejecuta todos los complementos “After Windows is ready” simultáneamente.
   - Amazon CloudWatch Logs
   - UserData
   - AWS Systems Manager (Systems Manager)

Para obtener más información acerca de los complementos de Windows, consulte Configuración de una instancia de Windows mediante el servicio EC2Config (heredado).

Ejecución de Sysprep con el servicio EC2Config

Utilice el siguiente procedimiento para crear una AMI estandarizada mediante Sysprep y el servicio EC2Config.

1. En la consola de Amazon EC2, localice o cree una AMI que desee duplicar.
2. Lance y conéctese a la instancia de Windows.
3. Personalícela.
4. Especifique los valores de configuración en el archivo de respuestas del servicio EC2Config:

   ```
   C:\Program Files\Amazon\Ec2ConfigService\sysprep2008.xml
   ```
5. En el menú Start de Windows, elija All Programs y, a continuación, elija EC2ConfigService Settings.
6. Elija la pestaña Image del cuadro de diálogo Ec2 Service Properties. Para obtener más información acerca de las opciones y la configuración del cuadro de diálogo de Ec2 Service Properties, consulte Ec2 Service Properties.
7. Seleccione una opción para la contraseña del administrador y, a continuación, seleccione Shutdown with Sysprep o Shutdown without Sysprep. EC2Config edita los archivos de configuración en función de la opción que haya seleccionado para la contraseña.
   - Random: EC2Config genera una contraseña, la cifra con la clave del usuario y muestra la contraseña cifrada a la consola. Esta configuración se deshabilita tras la primera inicialización para que esta contraseña persista si la instancia se reinicia o si se detiene y se vuelve a iniciar.
   - Specify: la contraseña se almacena en el archivo de respuestas de Sysprep en formato no cifrado (texto sin cifrar). Cuando Sysprep vuelve a ejecutarse, establece la contraseña del administrador. Si apaga en equipo en este momento, la contraseña se establece inmediatamente. Al volver a iniciarse el servicio, se elimina la contraseña del administrador. Es importante recordar esta contraseña, ya que no podrá volver a recuperarla.
   - Keep Existing: La contraseña existente para la cuenta de administrador no cambia al ejecutar Sysprep o al reiniciar EC2Config. Es importante recordar esta contraseña, ya que no podrá volver a recuperarla.
8. Seleccione OK.

Cuando se le solicite que confirme que desea ejecutar Sysprep y cerrar la instancia, haga clic en Yes. Verá que EC2Config ejecuta Sysprep. A continuación, se cierra la sesión en la instancia y esta se cierra. Si comprueba la página Instancias en la consola de Amazon EC2, el estado de la instancia

cambia de `Running` a `Stopping` y, finalmente, a `Stopped`. En este momento, es seguro crear una AMI desde esta instancia.

Puede invocar la herramienta Sysprep manualmente desde la línea de comando utilizando el siguiente comando:

```
"%programfiles%\amazon\ec2configservice\"ec2config.exe -sysprep""
```

> **Note**
>
> Las comillas dobles del comando no son necesarias si el shell del CMD ya está en el directorio C:\Program Files\Amazon\EC2ConfigService\.

No obstante, debe prestar especialmente atención para asegurarse de que las opciones del archivo XML especificadas en la carpeta `Ec2ConfigService\Settings` sean correctas, ya que, en caso contrario, es posible que no pueda conectarse a la instancia. Para obtener más información sobre los archivos de configuración, consulte Archivos de configuración de EC2Config. Para ver un ejemplo de cómo configurar y ejecutar Sysprep desde la línea de comando, consulte `Ec2ConfigService\Scripts\InstallUpdates.ps1`.

Modificar una AMI de

Puede modificar un conjunto limitado de atributos de Imagen de máquina de Amazon (AMI), como la descripción de la AMI y las propiedades de uso compartido. Sin embargo, el contenido de la AMI (datos binarios de volumen) no se puede modificar. Para modificar el contenido de la AMI, debe crear una AMI nueva.

> **Important**
>
> No puede modificar el contenido (datos binarios de volumen) de una AMI respaldada por EBS porque las instantáneas que las respaldan son inmutables. Tampoco puede modificar el contenido (datos binarios de volumen) de una AMI de Linux respaldada por el almacén de instancias (respaldada por S3) porque el contenido está firmado y se producirá un error en la inicialización de la instancia si las firmas no coinciden.

Para ver los atributos de la AMI que se pueden modificar, consulte ModifyImageAttribute en la referencia de la API de Amazon EC2.

En los siguientes temas se proporcionan instrucciones para usar la consola de Amazon EC2 y AWS CLI para modificar los atributos de una AMI:

- Convertir una AMI en pública
- Compartir una AMI con organizaciones o unidades organizativas específicas
- Compartir una AMI con cuentas de AWS específicas
- Usar el soporte de pago
- Configuración de la AMI

Copiar una AMI

Puede copiar una Imagen de máquina de Amazon (AMI) dentro de las regiones de AWS o entre ellas. Puede copiar las AMI basadas en Amazon EBS y las AMI basadas en almacén de instancias. Puede copiar las AMI basadas en EBS con instantáneas cifradas, y también cambiar el estado de cifrado durante el proceso de copia. Puede copiar las AMI que se compartieron con usted.

Si se copia una AMI de origen se obtiene una nueva AMI idéntica pero distinta, que también denominamos AMI de destino. La AMI de destino tiene su ID de AMI propio y único. Puede cambiar o cancelar el registro de la AMI de origen sin que ello afecte a la AMI de destino. y viceversa.

Con una AMI basada en EBS, cada una de las instantáneas con respaldo se copia en una instantánea de destino idéntica, pero distinta. Si copia una AMI en una región nueva, las instantáneas son copias completas (no incrementales). Si cifra instantáneas de copia de seguridad sin cifrar o las cifra en una nueva clave KMS, las instantáneas son copias completas (no incrementales). Las operaciones de copia posteriores de una AMI da como resultado copias incrementales de las instantáneas de copia de seguridad.

Contenido

- Cifrado y copias

Consideraciones

- Permiso para copiar AMI: puede utilizar las políticas de IAM para conceder o denegar a los usuarios el permiso para copiar las AMI. Los permisos de nivel de recursos especificados para la acción `CopyImage` solo se aplican a la nueva AMI. No se pueden especificar permisos de nivel de recursos para la AMI de origen.
- Permisos de inicialización y permisos de bucket de Amazon S3: AWS no copia los permisos de inicialización ni los permisos de bucket de Amazon S3 de la AMI de origen a la nueva AMI. Una vez que se haya completado la operación de copia, puede aplicar los permisos de inicialización y los permisos del bucket de Amazon S3 a la nueva AMI.
- Etiquetas: solo puede copiar las etiquetas de AMI definidas por el usuario que haya adjuntado a la AMI de origen. Las etiquetas del sistema (con el prefijo `aws:`) y las etiquetas definidas por el usuario que estén adjuntas por otras Cuentas de AWS no se copiarán. Al copiar una AMI, puede adjuntar nuevas etiquetas a la AMI de destino y a sus instantáneas de respaldo.

Costos

Copiar una AMI no supone ningún costo. Sin embargo, se aplican las tarifas estándar por almacenamiento y transferencia de datos. Si copia una AMI respaldada por EBS, se le cobrarán cargos por el almacenamiento de cualquier instantánea adicional de EBS.

Permisos de IAM

Para copiar una AMI basada en EBS o un almacén de instancias, necesita los siguientes permisos de IAM:

- `ec2:CopyImage`: para copiar la AMI. En el caso de las AMI basadas en EBS, también concede permiso para copiar las instantáneas de respaldo de la AMI.
- `ec2:CreateTags`: para etiquetar la AMI de destino. En el caso de las AMI basadas en EBS, también concede permiso para etiquetar las instantáneas de respaldo de la AMI de destino.

Si va a copiar una AMI basada en un almacén de instancias, necesitará los siguientes permisos de IAM adicionales:

- `s3:CreateBucket`: para crear el bucket de S3 en la región de destino para la nueva AMI

- `s3:GetBucketAcl`: para leer los permisos de ACL del bucket de origen
- `s3:ListAllMyBuckets`: para buscar un bucket de S3 existente para las AMI en la región de destino
- `s3:GetObject`: para leer los objetos del bucket de origen
- `s3:PutObject`: para escribir los objetos en el bucket de destino
- `s3:PutObjectAcl`: para escribir los permisos de los nuevos objetos en el bucket de destino

Ejemplo de política de IAM para copiar una AMI basada en EBS y etiquetar la AMI de destino y las instantáneas

El siguiente ejemplo de política le concede permiso para copiar cualquier AMI basada en EBS y etiquetar la AMI de destino y sus instantáneas de respaldo.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "PermissionToCopyAllImages",
        "Effect": "Allow",
        "Action": [
            "ec2:CopyImage",
            "ec2:CreateTags"
        ],
        "Resource": "arn:aws:ec2:*::image/*"
    }]
}
```

Ejemplo de política de IAM para copiar una AMI basada en EBS, pero que deniega el etiquetado de las nuevas instantáneas

El permiso `ec2:CopySnapshot` se concede automáticamente cuando se obtiene el permiso `ec2:CopyImage`. Esto incluye el permiso para etiquetar las nuevas instantáneas de respaldo de la AMI de destino. Se puede denegar explícitamente el permiso para etiquetar las nuevas instantáneas de respaldo.

La siguiente política de ejemplo le concede permiso para copiar cualquier AMI basada en EBS, pero le deniega etiquetar las nuevas instantáneas de respaldo de la AMI de destino.

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:CopyImage",
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*::image/*"
        },
        {
            "Effect": "Deny",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:::snapshot/*"
        }
    ]
}
```

Ejemplo de política de IAM para copiar una AMI basada en un almacén de instancias y etiquetar la AMI de destino

La siguiente directiva de ejemplo le concede permiso para copiar cualquier AMI basada en almacén de instancias en el bucket de origen especificado a la región especificada, y etiquetar la AMI de destino.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "PermissionToCopyAllImages",
            "Effect": "Allow",
            "Action": [
                "ec2:CopyImage",
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*::image/*"
        },
        {
            "Effect": "Allow",
            "Action": "s3:ListAllMyBuckets",
            "Resource": [
                "arn:aws:s3:::*"
            ]
        },
        {
            "Effect": "Allow",
```

```
            "Action": "s3:GetObject",
            "Resource": [
                "arn:aws:s3:::ami-source-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:GetBucketAcl",
                "s3:PutObjectAcl",
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::amis-for-account-in-region-hash"
            ]
        }
    ]
}
```

Para localizar el nombre de recurso de Amazon (ARN) del bucket de origen de la AMI, abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/ y, en el panel de navegación, elija AMI y busque el nombre del bucket en la columna Origen.

> **Note**
>
> El permiso `s3:CreateBucket` solo es necesario la primera vez que copia una AMI basada en un almacén de instancias en una región individual. Después de eso, el bucket de Amazon S3 que ya se ha creado en la región se utiliza para almacenar todas las AMIs futuras que se copian en esa región.

Copiar una AMI

Puede copiar una AMI mediante la AWS Management Console, la AWS Command Line Interface, los SDK o la API de Amazon EC2, todos los cuales admiten la acción `CopyImage`.

Console

Para copiar una AMI

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

2. Desde la barra de navegación de la consola, seleccione la región que contiene la AMI.
3. En el panel de navegación, elija AMI para mostrar la lista de AMI disponibles en la región.
4. Si no ve la AMI que desea copiar, elija otro filtro. Puede filtrar según las AMI: De mi propiedad, Imágenes privadas, Imágenes públicas e Imágenes deshabilitadas.
5. Seleccione la AMI que desea copiar y elija Acciones y, a continuación, Copiar AMI.
6. En la página Copiar AMI, especifique la siguiente información:

    a. Nombre de copia de AMI: el nombre para la nueva AMI. Puede incluir la información del sistema operativo en el nombre porque Amazon EC2 no proporciona esta información cuando muestra detalles sobre la AMI.

    b. Descripción de copia de AMI: de forma predeterminada, la descripción incluye información acerca de la AMI de origen para que pueda diferenciar la copia de la original. Puede cambiar esta descripción según sea necesario.

    c. Región de destino: indica la región en la que desea copiar la AMI. Para obtener más información, consulte Copias entre regiones.

    d. Copiar etiquetas: active esta casilla de verificación para incluir las etiquetas de AMI definidas por el usuario al copiar la AMI. Las etiquetas del sistema (con el prefijo `aws:`) y las etiquetas definidas por el usuario que estén adjuntas por otras Cuentas de AWS no se copiarán.

    e. (Solo AMI basadas en EBS) Cifrar instantáneas de EBS de una copia de AMI: seleccione esta casilla para cifrar las instantáneas de destino o para volver a cifrarlas con una clave diferente. Si se habilita el cifrado de manera predeterminada, la casilla Cifrar instantáneas de EBS de una copia de AMI se selecciona y no se puede desactivar. Para obtener más información, consulte Cifrado y copias.

    f. (Solo AMI basadas en EBS) Clave de KMS: la clave de KMS que se utilizará para cifrar las instantáneas de destino.

    g. Etiquetas: puede etiquetar la AMI y las instantáneas con las mismas etiquetas o con etiquetas diferentes.

        - Para etiquetar la AMI nueva y las instantáneas nuevas con las mismas etiquetas, elija Etiquetar imagen e instantáneas juntas. Las mismas etiquetas se aplican a la AMI nueva y a todas las instantáneas que se crean.
        - Para etiquetar la AMI nueva y las instantáneas nuevas con etiquetas diferentes, elija Etiquetar imagen e instantáneas por separado. Se aplican diferentes etiquetas a la AMI nuevas y a las instantáneas que se crean. Sin embargo, tenga en cuenta que

todas las instantáneas nuevas que se crean obtienen las mismas etiquetas. No puede etiquetar cada instantánea nueva con una etiqueta diferente.

Para agregar una etiqueta, elija Agregar etiqueta y especifique la clave y el valor de la etiqueta. Repita este proceso para cada etiqueta.

h. Cuando lo tenga todo listo para copiar la AMI, seleccione Copiar AMI.

El estado inicial de la nueva AMI es `Pending`. La operación de copia de la AMI finaliza cuando el estado es `Available`.

AWS CLI

Para copiar una AMI con la AWS CLI

Puede copiar una AMI mediante el comando copy-image. Debe especificar tanto la región de origen como la de destino. La región de origen se especifica mediante el parámetro `--source-region`. La región de destino se especifica mediante el parámetro `--region` o bien mediante una variable de entorno. Para obtener más información, consulte el tema sobre configuración de la interfaz de línea de comandos de AWS.

(Solo AMI basadas en EBS) Al cifrar una instantánea de destino durante la copia, debe especificar estos parámetros adicionales: `--encrypted` y `--kms-key-id`.

Para ver ejemplos de comandos, consulte Ejemplos en la sección copy-image de la Referencia de comandos de AWS CLI.

PowerShell

Para copiar una AMI mediante la Tools for Windows PowerShell

Puede copiar una AMI mediante el comando Copy-EC2Image. Debe especificar tanto la región de origen como la de destino. La región de origen se especifica mediante el parámetro `-SourceRegion`. La región de destino se especifica mediante el parámetro `-Region` o bien mediante el comando `Set-AWSDefaultRegion`. Para obtener más información, consulte Especificación de regiones de AWS.

(Sólo AMI basadas en EBS) Al cifrar una instantánea de destino durante la copia, debe especificar estos parámetros adicionales: `-Encrypted` y `-KmsKeyId`.

Detener una operación de copia de una AMI pendiente

Puede detener la copia de una AMI pendiente con la AWS Management Console o la línea de comandos.

Console

Para parar una operación de copia de una AMI mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la barra de navegación, seleccione la región de destino desde el selector de regiones.
3. En el panel de navegación, elija AMIs.
4. Seleccione la AMI cuya copia desea detener y elija Acciones y, a continuación, Anular registro de la AMI.
5. Cuando se le solicite la confirmación, elija Anular registro de AMI.

Command line

Para parar una operación de copia de una AMI con la línea de comando

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

- deregister-image (AWS CLI)
- Unregister-EC2Image (AWS Tools for Windows PowerShell)

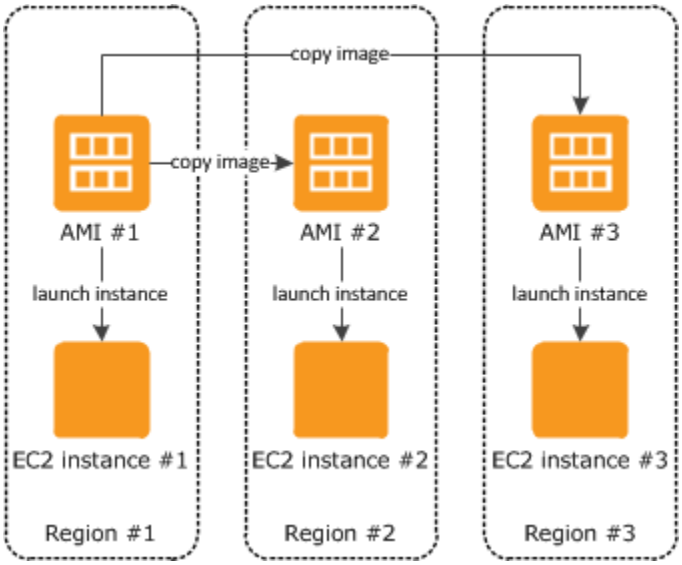
Copias entre regiones

El copiado de una AMI entre regiones geográficamente distribuidas proporciona los siguientes beneficios:

- Implementación global coherente: al copiar una AMI de una región en otra, puede iniciar instancias coherentes basadas en la misma AMI en regiones diferentes.
- Escalabilidad: puede diseñar y construir más fácilmente aplicaciones globales para satisfacer las necesidades de los usuarios, con independencia de su ubicación.
- Desempeño: puede mejorar el desempeño distribuyendo la aplicación, así como localizando componentes fundamentales de esta más próximos a los usuarios. También puede aprovechar las características específicas para cada región, como tipos de instancia u otros servicios de AWS.

- Alta disponibilidad: puede diseñar e implementar aplicaciones entre regiones de AWS para aumentar la disponibilidad.

En el siguiente diagrama, se muestra la relación entre una AMI de origen y dos AMI copiadas en diferentes regiones, además de las instancias de EC2 iniciadas desde cada una de ellas. Al iniciar una instancia desde una AMI, esta reside en la misma región en la que reside la AMI. Si realiza cambios en la AMI de origen y desea que estos se reflejen en las imágenes de tipo AMIs de las regiones de destino, debe volver a copiar la AMI de origen en las regiones de destino.



Al copiar por primera vez una AMI con respaldo en el almacén de instancias en una región, se crea un bucket de Amazon S3 para las imágenes de tipo AMIs copiadas en dicha región. Todas las imágenes de tipo AMIs con respaldo en el almacén de instancias que copie en esa región se almacenan en dicho bucket. Los nombres de los buckets tienen el siguiente formato: amis-for-*cuenta*-in-*región*-*hash*. Por ejemplo: `amis-for-123456789012-in-us-east-2-yhjmxvp6`.

Requisito previo

Antes de copiar una AMI, debe asegurarse de que el contenido de la AMI de origen esté actualizado para poder ser ejecutado en una región diferente. Por ejemplo, deberá actualizar las cadenas de conexión de la base de datos o cualquier otro dato de configuración de la aplicación para que se asocien a los recursos adecuados. De lo contrario, es posible que las instancias iniciadas desde la AMI nueva en la región de destino aún usen los recursos de la región de origen, lo cual puede afectar al rendimiento y al costo.

Limitaciones

- Las regiones de destino se limitan a 100 copias de AMI simultáneas.
- No puede copiar una AMI paravirtual (PV) en una región que no admite AMI PV. Para obtener más información, consulte Tipos de virtualización de AMI.

Copias entre cuentas

Puede compartir una AMI con otra cuenta de AWS. Compartir una AMI no afecta a la propiedad de dicha AMI. Los cargos de almacenamiento en la región se cobran a la cuenta propietaria. Para obtener más información, consulte Compartir una AMI con cuentas de AWS específicas.

Si copia una AMI que se ha compartido en su cuenta, será el propietario de la AMI de destino en su cuenta. Al propietario de la AMI de origen se le cobrarán las tarifas de transferencia estándar de Amazon EBS o Amazon S3 y a usted se le cobrará por el almacenamiento de la AMI de destino en la región de destino.

Permisos de recursos

Para copiar una AMI compartida con usted desde otra cuenta, el propietario de la AMI de origen debe concederle permisos de lectura para el almacenamiento que respalda a esta AMI. El almacenamiento es la instantánea de EBS asociada (para una AMI basada en Amazon EBS) o un bucket de S3 asociado (para una AMI basada en un almacén de instancias). Si la AMI compartida tiene instantáneas cifradas, el propietario también debe compartir la clave o claves con usted. Para obtener más información sobre la concesión de permisos de recursos, para las snapshots de EBS, consulte Compartir una instantánea de Amazon EBS en la Guía del usuario de Amazon EBS, y para los buckets de S3, consulte Identity and Access Management en Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

> **Note**
>
> Para copiar una AMI con sus etiquetas, debe tener permisos de inicialización para la AMI de origen.

Cifrado y copias

En la siguiente tabla se muestra la compatibilidad con cifrado para diversos escenarios de copia de AMI. Si bien es posible copiar una instantánea sin cifrar para obtener una instantánea cifrada, no se puede copiar una instantánea cifrada para obtener una sin cifrar.

Escenario	Descripción	Soportado
1	De una sin cifrar a otra sin cifrar	Sí
2	De una cifrada a otra cifrada	Sí
3	De una sin cifrar a otra cifrada	Sí
4	De una cifrada a otra sin cifrar	No

> **Note**
>
> El cifrado durante la acción `CopyImage` solo se aplica a las imágenes de tipo AMIs con respaldo Amazon EBS. Puesto que una AMI con respaldo en el almacén de instancias no se basa en instantáneas, no puede usar la copia para cambiar su estado de cifrado.

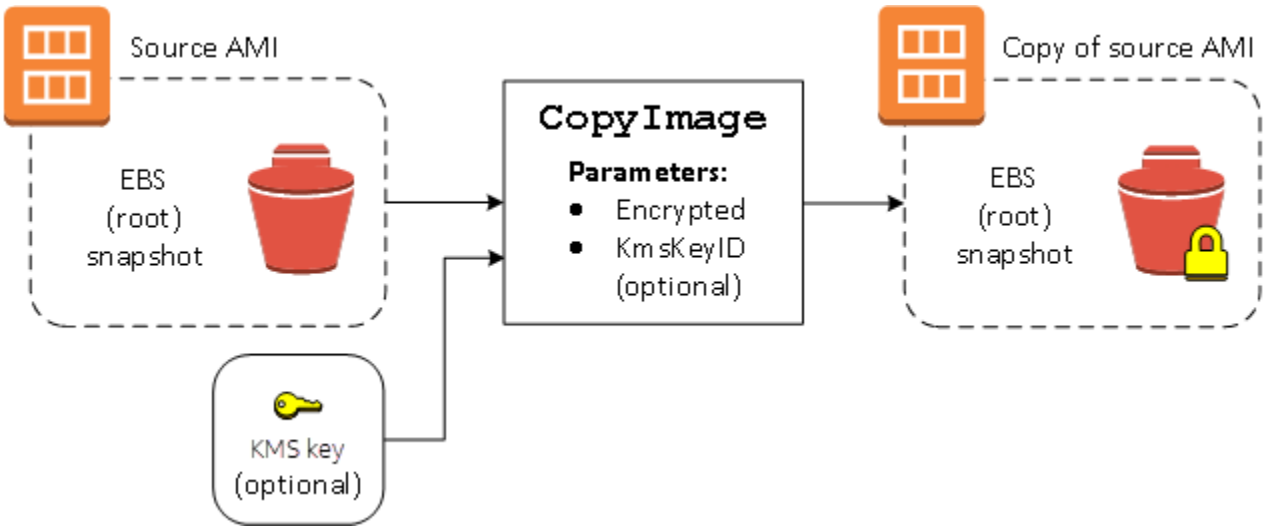
De forma predeterminada (es decir, sin especificar los parámetros de cifrado), la instantánea respaldada de una AMI se copia con su estado de cifrado original. Al copiar una AMI respaldada por una instantánea sin cifrar se obtiene una instantánea de destino idéntica que tampoco está cifrada. Si la AMI de origen está respaldada por una instantánea cifrada, cuando se copia se obtiene una instantánea de destino idéntica que se cifra con la misma clave de AWS KMS. Al copiar una AMI respaldada por varias instantáneas, de forma predeterminada, se conserva el estado de cifrado de origen en cada una de las instantáneas de destino.

Si especifica los parámetros de cifrado mientras copia una AMI, puede cifrar o volver a cifrar sus instantáneas respaldadas. El siguiente ejemplo muestra un caso no predeterminado que aporta parámetros de cifrado a la acción `CopyImage` para cambiar el estado de cifrado de la AMI del objetivo.

Copia de una AMI de origen sin cifrar en una AMI de destino cifrada

En este caso, una AMI respaldada por una instantánea raíz no cifrada se copia en una AMI con una instantánea raíz cifrada. La acción `CopyImage` se invoca con dos parámetros de cifrado, incluida una clave administrada por el cliente. Como resultado, el estado de cifrado de la instantánea raíz cambia, de modo que la AMI de destino se respalda por una instantánea raíz que contiene los mismos datos que la instantánea de origen, pero cifrada con la clave especificada. Usted incurre en costos de almacenamiento de las instantáneas en ambas AMI, así como en cargos correspondientes a las instancias que lance desde cualquiera de las AMI.

> **Note**
>
> Habilitar el cifrado de forma predeterminada tiene el mismo efecto que configurar el parámetro `Encrypted` en `true` para todas las instantáneas de la AMI.



La configuración del parámetro `Encrypted` cifra la única instantánea para esta instancia. Si no especifica el parámetro `KmsKeyId`, la clave predeterminada administrada por el cliente se utiliza para cifrar la copia de la instantánea.

Para obtener más información acerca de la copia de AMIs con instantáneas cifradas, consulte Usar el cifrado con las AMI con respaldo de EBS.

Almacenar y restaurar una AMI mediante S3

Puede almacenar una Imagen de máquina de Amazon (AMI) en un bucket de Amazon S3, copiar la AMI en otro bucket de S3 y, a continuación, restaurarla desde el bucket de S3. Al almacenar y restaurar una AMI usando buckets de S3, puede copiar AMI de una partición de AWS a otra, por

ejemplo, desde la partición comercial principal a la partición AWS GovCloud (US). También puede hacer copias de archivo de AMI almacenándolas en un bucket de S3.

Las API admitidas para almacenar y restaurar una AMI usando S3 son `CreateStoreImageTask`, `DescribeStoreImageTasks` y `CreateRestoreImageTask`.

`CopyImage` es la API recomendada para copiar AMI dentro de una partición de AWS. Sin embargo, `CopyImage` no puede copiar una AMI a otra partición.

Para obtener información sobre las particiones de AWS, consulte *`partición`* en la página Nombres de recursos de Amazon (ARN) de la Guía del usuario de IAM.

> **Warning**
>
> Asegúrese de que cumple con todas las leyes y requisitos empresariales aplicables al mover datos entre particiones de AWS o regiones de AWS, incluyendo, entre otros, cualquier normativa gubernamental aplicable y requisitos de residencia de datos.

Temas

Casos de uso

Utilice las API de almacenamiento y restauración para hacer lo siguiente:

- Copiar una AMI de una partición de AWS a otra partición de AWS
- Hacer copias de archivo de AMI

Copiar una AMI de una partición de AWS a otra partición de AWS

Al almacenar y restaurar una AMI mediante buckets S3, puede copiar una AMI de una partición de AWS a otra, o de una región de AWS a otra. En el siguiente ejemplo, copia una AMI de la partición comercial principal a la partición de AWS GovCloud (US), específicamente desde la región `us-east-2` hacia la región `us-gov-east-1`.

Para copiar una AMI de una partición a otra, siga estos pasos:

- Almacene la AMI en un bucket de S3 en la región actual mediante `CreateStoreImageTask`. En este ejemplo, el bucket de S3 se encuentra en `us-east-2`. Para obtener un comando de ejemplo, consulte Almacenar una AMI en un bucket de S3.
- Supervise el progreso de la tarea de almacén mediante `DescribeStoreImageTasks`. El objeto se vuelve visible en el bucket de S3 cuando se completa la tarea. Para obtener un comando de ejemplo, consulte Describir el progreso de una tarea de almacén de AMI.
- Copie el objeto AMI almacenado en un bucket de S3 en la partición de destino mediante un procedimiento que elija. En este ejemplo, el bucket de S3 se encuentra en `us-gov-east-1`.

  > **Note**
  >
  > Debido a que necesita credenciales de AWS diferentes para cada partición, no puede copiar un objeto de S3 directamente de una partición a otra. El proceso para copiar un objeto de S3 a través de particiones está fuera del ámbito de esta documentación. Proporcionamos los siguientes procesos de copia como ejemplos, pero debe utilizar el proceso de copia que cumpla con los requisitos de seguridad.
  >
  > - Para copiar una AMI entre particiones, el proceso de copiado podría ser tan sencillo como el siguiente: descargue el objeto desde el bucket de origen a un host intermedio (por ejemplo, una instancia de EC2 o computadora personal) y, a continuación, cargue el objeto desde el host al bucket de destino. Para cada etapa del proceso, utilice las credenciales de AWS de la partición.
  > - Para un uso más constante, considere la posibilidad de desarrollar una aplicación que administre las copias, posiblemente al utilizar descargas y cargas multiparte de S3.

- Restaure la AMI desde el bucket de S3 en la partición de destino mediante `CreateRestoreImageTask`. En este ejemplo, el bucket de S3 se encuentra en `us-gov-east-1`. Para obtener un comando de ejemplo, consulte Restaurar una AMI desde un bucket de S3.

- Supervise el progreso de la tarea de restauración describiendo la AMI para verificar cuando su estado esté disponible. También puede supervisar los porcentajes de progreso de las instantáneas que componen la AMI restaurada describiendo las instantáneas.

Hacer copias de archivo de AMI

Puede hacer copias de archivo de AMI almacenándolas en un bucket de S3. Para obtener un comando de ejemplo, consulte Almacenar una AMI en un bucket de S3.

La AMI se empaqueta en un solo objeto en S3 y todos los metadatos AMI (excluyendo la información compartida) se conservan como parte de la AMI almacenada. Los datos de AMI se comprimen como parte del proceso de almacenamiento. Las AMI que contienen datos que se pueden comprimir fácilmente darán como resultado objetos más pequeños en S3. Para reducir costos, puede utilizar niveles de almacenamiento S3 menos costosos. Para obtener más información, consulte las clases de almacenamiento de Amazon S3 y los precios de Amazon S3

Cómo funcionan las API de almacenamiento y restauración de AMI

Para almacenar y restaurar una AMI mediante S3, utilice las siguientes API:

- `CreateStoreImageTask` – Almacena la AMI en un bucket de S3
- `DescribeStoreImageTasks` – Proporciona el progreso de la tarea de almacenamiento de AMI
- `CreateRestoreImageTask` – Restaura la AMI desde un bucket de S3

Cómo funcionan las API

- CreateStoreImageTask
- DescribeStoreImageTasks
- CreateRestoreImageTask

CreateStoreImageTask

La API CreateStoreImageTask almacena una AMI como un único objeto en un bucket de S3.

La API crea una tarea que lee todos los datos de la AMI y sus instantáneas y, a continuación, utiliza una carga multiparte de S3 para almacenar los datos en un objeto S3. La API toma todos los componentes de la AMI, incluida la mayoría de los metadatos AMI no específicos de la región, y todas las instantáneas de EBS contenidas en la AMI, y los empaqueta en un único objeto en S3. Los

datos se comprimen como parte del proceso de carga para reducir la cantidad de espacio utilizado en S3, por lo que el objeto en S3 podría ser menor que la suma de los tamaños de las instantáneas en la AMI.

Si hay etiquetas AMI y de instantáneas visibles para la cuenta que llama a esta API, se conservan.

El objeto en S3 tiene el mismo ID que la AMI, pero con una extensión `.bin`. Los siguientes datos también se almacenan como etiquetas de metadatos S3 en el objeto S3: nombre de AMI, descripción de AMI, fecha de registro de AMI, cuenta de propietario de AMI y una marca de hora para la operación de almacén.

El tiempo que se tarda en completar la tarea depende del tamaño de la AMI. También depende de cuántas otras tareas estén en curso dado que las tareas están en cola. Puede realizar un seguimiento del progreso de la tarea llamando a la API DescribeStoreImageTasks.

La suma de los tamaños de todas las AMI en curso está limitada a 600 GB de datos de instantáneas de EBS por cuenta. Se rechazará la creación de tareas adicionales hasta que las tareas en curso sean inferiores al límite. Por ejemplo, si se está almacenando una AMI con 100 GB de datos de instantáneas y otra AMI con 200 GB de datos de instantáneas, se aceptará otra solicitud, dado que el total en curso es de 300 GB, que es menor que el límite. Sin embargo, si una sola AMI con 800 GB de datos de instantáneas se está almacenando actualmente, se rechazan otras tareas hasta que se complete la tarea.

DescribeStoreImageTasks

La API DescribeStoreImageTasks describe el progreso de las tareas del almacén de AMI. Puede describir tareas para AMI especificadas. Si no especifica AMI, obtendrá una lista paginada de todas las tareas de imagen de almacén que se han procesado en los últimos 31 días.

Para cada tarea AMI, la respuesta indica si la tarea es `InProgress`, `Completed` o `Failed`. En el caso de las tareas `InProgress`, la respuesta muestra un progreso estimado como porcentaje.

Las tareas se enumeran en orden cronológico inverso.

Actualmente, solo se pueden ver las tareas del mes anterior.

CreateRestoreImageTask

La API CreateStoreImageTask inicia una tarea que restaura una AMI de un objeto S3 que se creó previamente mediante una solicitud CreateStoreImageTask.

La tarea de restauración se puede realizar en la misma región o en una región diferente en la que se realizó la tarea de almacenamiento.

El bucket de S3 desde el que se restaurará el objeto AMI debe estar en la misma región en la que se solicita la tarea de restauración. La AMI será restaurada en esta Región.

La AMI se restaura con sus metadatos, como el nombre, la descripción y las asignaciones de dispositivos de bloque correspondientes a los valores de la AMI almacenada El nombre debe ser único para las AMI de la región de esta cuenta. Si no proporciona un nombre, la nueva AMI obtiene el mismo nombre que la AMI original. La AMI obtiene un nuevo ID de AMI que se genera en el momento del proceso de restauración.

El tiempo que se tarda en completar la tarea de restauración de la AMI depende del tamaño de la AMI. También depende de cuántas otras tareas estén en curso dado que las tareas están en cola. Puede ver el progreso de la tarea describiendo la AMI (describe-images) o sus instantáneas de EBS (describe-snapshots). Si la tarea falla, la AMI y las instantáneas se mueven a un estado de error.

La suma de los tamaños de todas las AMI en curso está limitada a 300 GB (según el tamaño después de la restauración) de los datos de instantáneas de EBS por cuenta. Se rechazará la creación de tareas adicionales hasta que las tareas en curso sean inferiores al límite.

Limitaciones

- Para almacenar una AMI, su Cuenta de AWS debe ser propietaria de la AMI y sus instantáneas, o bien la AMI y sus instantáneas deben compartirse directamente con su cuenta. No puede almacenar una AMI si solo se comparte públicamente.
- Solo se pueden almacenar AMI respaldadas por EBS usando estas API.
- No se admiten AMI paravirtuales (PV).
- El tamaño de una AMI (antes de la compresión) que se puede almacenar está limitado a 5000 GB.
- Cuota en solicitudes de imágenes de almacén: 600 GB de trabajo de almacenamiento (datos de instantáneas) en curso.
- Cuota en solicitudes de imagen de restauración: 300 GB de trabajo de restauración (datos de instantáneas) en curso.
- Durante la tarea de almacenamiento, las instantáneas no deben eliminarse y la entidad principal de IAM que realiza el almacén debe tener acceso a las instantáneas; de lo contrario, el proceso de almacenamiento fallará.
- No puede crear varias copias de una AMI en el mismo bucket de S3.

- Una AMI almacenada en un bucket de S3 no se puede restaurar con su ID de AMI original. Puede mitigar esto mediante el uso de alias AMI.
- En la actualidad, las API de almacenamiento y restauración solo se admiten mediante el uso de AWS Command Line Interface, AWS SDK y la API de Amazon EC2. No se puede almacenar ni restaurar una AMI mediante la consola de Amazon EC2.

Costos

Cuando almacena y restaura AMI mediante S3, se le cobran los servicios que utilizan las API de almacenamiento y restauración, así como por la transferencia de datos. Las API utilizan S3 y EBS Direct API (utilizadas internamente por estas API para acceder a los datos de instantáneas). Para obtener más información, consulte Precios de Amazon S3 y Precios de Amazon EBS.

Protección de sus AMI

Para utilizar las API de almacenamiento y restauración, el bucket de S3 y la AMI deben estar en la misma región. Es importante asegurarse de que el bucket de S3 esté configurado con la seguridad suficiente para proteger el contenido de la AMI y que la seguridad se mantenga mientras los objetos AMI permanezcan en el bucket. Si esto no se puede hacer, no se recomienda el uso de estas API. Asegúrese de que el acceso público al bucket de S3 no está permitido. Recomendamos habilitar el cifrado del lado del servidor para los buckets de S3 en los que almacena las AMI, aunque no es necesario.

Para obtener información acerca de cómo establecer la configuración de seguridad adecuada para los buckets de S3, consulte los siguientes temas de seguridad:

- bloquear el acceso público al almacenamiento de Amazon S3
- Establecer el comportamiento predeterminado del cifrado del lado del servidor para los buckets de Amazon S3
- ¿Qué política de bucket de S3 debo utilizar para cumplir la regla s3-bucket-ssl-requests-only de AWS Config?
- Habilitar el registro de acceso al servidor de Amazon S3

Cuando las instantáneas de AMI se copian en el objeto de S3, los datos se copian a través de conexiones TLS. Puede almacenar AMI con instantáneas cifradas, pero las instantáneas se descifran como parte del proceso de almacenamiento.

Permisos para almacenar y restaurar AMI mediante S3

Si sus entidades principales de IAM van a almacenar o restaurar AMI usando Amazon S3, debe concederles los permisos necesarios.

En la siguiente política de ejemplo se incluyen todas las acciones necesarias para permitir que una entidad principal de IAM lleve a cabo las tareas de almacenamiento y restauración.

También puede crear políticas de IAM que otorguen a las entidades principales acceso solo a recursos específicos. Para obtener más políticas de ejemplo, vea Administración de acceso para los recursos de AWS en la Guía del usuario de IAM.

> **Note**
>
> Si las instantáneas que componen la AMI están cifradas o si su cuenta está habilitada para el cifrado de forma predeterminada, la entidad principal de IAM debe tener permiso para usar la clave de KMS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:DeleteObject",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:PutObject",
                "s3:PutObjectTagging",
                "s3:AbortMultipartUpload",
                "ebs:CompleteSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:ListChangedBlocks",
                "ebs:ListSnapshotBlocks",
                "ebs:PutSnapshotBlock",
                "ebs:StartSnapshot",
                "ec2:CreateStoreImageTask",
                "ec2:DescribeStoreImageTasks",
                "ec2:CreateRestoreImageTask",
                "ec2:GetEbsEncryptionByDefault",
                "ec2:DescribeTags",
```

```
                "ec2:CreateTags"
            ],
            "Resource": "*"
        }
    ]
}
```

Trabajar con el almacén de AMI y restaurar las API

Temas

- Almacenar una AMI en un bucket de S3
- Describir el progreso de una tarea de almacén de AMI
- Restaurar una AMI desde un bucket de S3

Almacenar una AMI en un bucket de S3

Para almacenar una AMI (AWS CLI)

Utilice el comando create-store-image-task. Especifique el ID de la AMI y el nombre del bucket de S3 en el que desea almacenar la AMI.

```
aws ec2 create-store-image-task \
    --image-id ami-1234567890abcdef0 \
    --bucket myamibucket
```

Salida prevista

```
{
  "ObjectKey": "ami-1234567890abcdef0.bin"
}
```

Describir el progreso de una tarea de almacén de AMI

Para describir el progreso de una tarea de almacén de AMI (AWS CLI)

Utilice el comando describe-store-image-tasks.

```
aws ec2 describe-store-image-tasks
```

Salida prevista

```
{
  "AmiId": "ami-1234567890abcdef0",
  "Bucket": "myamibucket",
  "ProgressPercentage": 17,
  "S3ObjectKey": "ami-1234567890abcdef0.bin",
  "StoreTaskState": "InProgress",
  "StoreTaskFailureReason": null,
  "TaskStartTime": "2021-01-01T01:01:01.001Z"
}
```

Restaurar una AMI desde un bucket de S3

Para restaurar una AMI (AWS CLI)

Utilice el comando create-restore-image-task. Utilizando los valores para `S3ObjectKey` y `Bucket` desde la salida `describe-store-image-tasks`, especifique la clave de objeto de la AMI y el nombre del bucket de S3 en el que se copió la AMI. Especifique también un nombre para la AMI restaurada. El nombre debe ser único para las AMI de la región de esta cuenta.

> **Note**
>
> La AMI restaurada obtiene un nuevo ID de AMI.

```
aws ec2 create-restore-image-task \
    --object-key ami-1234567890abcdef0.bin \
    --bucket myamibucket \
    --name "New AMI Name"
```

Resultado previsto

```
{
   "ImageId": "ami-0eab20fe36f83e1a8"
}
```

Uso de rutas de archivos en S3

Puede utilizar las rutas de archivos al almacenar y restaurar las AMI de la siguiente manera:

- Al almacenar una AMI en S3, la ruta del archivo se puede agregar al nombre del bucket. Internamente, el sistema separa la ruta del nombre del bucket y, a continuación, agrega la ruta a la clave de objeto que se genera para almacenar la AMI. La ruta de objeto completa se muestra en la respuesta de la llamada a la API.
- Al restaurar la AMI, dado que hay un parámetro de clave de objeto disponible, la ruta se puede agregar al principio del valor de la clave de objeto.

Puede utilizar las rutas de archivos cuando utilice la AWS CLI y los SDK.

Ejemplo: uso de una ruta de archivo al almacenar y restaurar una AMI (AWS CLI)

En el siguiente ejemplo se almacena primero una AMI en S3, con la ruta de archivo agregada al nombre del bucket. A continuación, en el ejemplo se restaura la AMI desde S3, con la ruta de archivo antepuesta al parámetro de clave de objeto.

1. Guarde la AMI. Para `--bucket`, especifique la ruta de archivo después del nombre del bucket, de la siguiente manera:

   ```
   aws ec2 create-store-image-task \
       --image-id ami-1234567890abcdef0 \
       --bucket myamibucket/path1/path2
   ```

   Resultado previsto

   ```
   {
     "ObjectKey": "path1/path2/ami-1234567890abcdef0.bin"
   }
   ```

2. Restaure la AMI. Para `--object-key`, especifique el valor de la salida del paso anterior, que incluye la ruta de archivo.

   ```
   aws ec2 create-restore-image-task \
       --object-key path1/path2/ami-1234567890abcdef0.bin \
       --bucket myamibucket \
       --name "New AMI Name"
   ```

Dar de baja una AMI

Puede dar de baja una AMI para indicar que está desactualizada y no debería utilizarse. También puede especificar una fecha de baja futura para una AMI para indicar cuándo estará desactualizada la AMI. Por ejemplo, puede dar de baja una AMI que ya no se mantiene activamente o que se ha reemplazado por una versión más reciente. De forma predeterminada, las AMI obsoletas no aparecen en las listas de AMI, lo que impide que los usuarios nuevos utilicen AMI desactualizadas. Sin embargo, los usuarios existentes y los servicios de inicialización, como las plantillas de inicialización y los grupos de Auto Scaling, pueden seguir utilizando una AMI obsoleta si especifican su ID. Para eliminar la AMI de modo que los usuarios y los servicios no puedan utilizarla, debe anular su registro.

Después de dar de baja una AMI:

- Para los usuarios de AMI, la AMI obsoleta no aparece en las llamadas a la API DescribeImages a menos que especifique su ID o especifique que las AMI obsoletas deben aparecer. Los propietarios de AMI siguen viendo AMI obsoletas en las llamadas a la API DescribeImages.
- Para los usuarios de AMI, la AMI obsoleta no está disponible para seleccionarse mediante la consola de EC2. Por ejemplo, una AMI obsoleta no aparece en el catálogo de AMI en el launch wizard de instancias. Los propietarios de las AMI siguen viendo AMI obsoletas en la consola de EC2.
- Para los usuarios de AMI, si conoce el ID de una AMI obsoleta, puede seguir iniciando instancias utilizando la AMI obsoleta mediante la API, la CLI o los SDK.
- Los servicios de inicialización, como plantillas de inicialización y grupos de Auto Scaling, pueden seguir haciendo referencia a AMI obsoletas.
- Las instancias de EC2 que se iniciaron mediante una AMI que posteriormente queda obsoleta no se ven afectadas y pueden detenerse, iniciarse y reiniciarse.

Puede dar de baja las AMI privadas y públicas.

También puede crear políticas de AMI respaldadas por EBS de Amazon Data Lifecycle Manager para automatizar la obsolescencia de las AMI respaldadas por EBS. Para obtener más información, consulte Automatización de los ciclos de vida de las AMI.

> **Note**
>
> De forma predeterminada, la fecha de obsolescencia de todas las AMI públicas se establece en dos años a partir de la fecha de creación de la AMI. Puede establecer una fecha de obsolescencia anterior a los dos años. Para anular la fecha de obsolescencia o para aplazarla, debe hacer que la AMI sea privada compartiéndola solo con cuentas de AWS específicas.

Temas

Costos

Cuando da de baja una AMI, esta no se elimina. El propietario de la AMI sigue pagando las instantáneas de la AMI. Para dejar de pagar las instantáneas, el propietario de la AMI debe eliminar la AMI anulando el registro.

Limitaciones

- Para dar de baja una AMI, debe ser el propietario de la AMI.

Dar de baja una AMI

Puede dar de baja una AMI en una fecha y hora específicas. Debe ser el propietario de la AMI para realizar este procedimiento.

Console

Para dar de baja una AMI en una fecha específica

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

2. En el panel de navegación izquierdo, elija AMI.
3. En la barra de filtros, elija Owned by me (De mi propiedad).
4. Seleccione la AMI y, a continuación, elija Actions, Administrar la obsolescencia de la AMI. Puede seleccionar varias AMI para establecer la misma fecha de obsolescencia de varias AMI al mismo tiempo.
5. Seleccione la casilla de verificación Habilitar y, a continuación, ingrese la fecha y la hora de obsolescencia.

   El límite superior para la fecha de obsolescencia es dentro de 10 años, excepto en el caso de las AMI públicas, donde el límite superior es de 2 años a partir de la fecha de creación. No puede especificar una fecha pasada.
6. Seleccione Guardar.

AWS CLI

Para dar de baja una AMI en una fecha específica

Utilice el comando enable-image-deprecation. Especifique el ID de la AMI y la fecha y hora en las que desea dar de baja la AMI. Si especifica un valor en segundos, Amazon EC2 redondea los segundos al minuto más cercano.

El límite superior para `deprecate-at` es dentro de 10 años, excepto en el caso de las AMI públicas, donde el límite superior es de 2 años a partir de la fecha de creación. No puede especificar una fecha pasada.

```
aws ec2 enable-image-deprecation \
    --image-id ami-1234567890abcdef0 \
    --deprecate-at "2021-10-15T13:17:12.000Z"
```

Resultado previsto

```
{
  "Return": "true"
}
```

Compruebe cuándo se utilizó una AMI por última vez

`LastLaunchedTime` es una marca de tiempo que indica cuándo se utilizó la AMI por última vez para iniciar una instancia. Las AMI que no se hayan utilizado recientemente para iniciar una instancia pueden ser buenas opciones para darlas de baja o anular su registro.

> **Note**
>
> - Cuando se utiliza una AMI para iniciar una instancia, hay una demora de 24 horas antes de que se informe del uso.
> - Los datos de `lastLaunchedTime` están disponibles a partir de abril de 2017.

Console

Para ver el momento de la última inicialización de una AMI

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación izquierdo, elija AMI.
3. En la barra de filtros, elija De mi propiedad.
4. Seleccione la AMI, y luego compruebe el campo Momento de la última inicialización (si ha seleccionado la casilla de verificación situada junto a la AMI, se encuentra en la pestaña Detalles. El campo muestra la fecha y la hora en que se utilizó la AMI por última vez para iniciar una instancia.

AWS CLI

Para ver el momento del último inicialización de una AMI

Ejecute el comando describe-image-attribute y especifique `--attribute lastLaunchedTime`. Debe ser el propietario de la AMI para ejecutar este comando.

```
aws ec2 describe-image-attribute \
    --image-id ami-1234567890example \
    --attribute lastLaunchedTime
```

Ejemplo de resultado

```
{
    "LastLaunchedTime": {
        "Value": "2022-02-10T02:03:18Z"
    },
    "ImageId": "ami-1234567890example",
}
```

Describir las AMI obsoletas

Puede ver la fecha y la hora de obsolescencia de una AMI y filtrar todas las AMI por dicha fecha. También puede utilizar la AWS CLI para detallar todas las AMI que se hayan dado de baja, cuya fecha de baja es una fecha pasada.

Console

Para ver la fecha de baja de una AMI

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación izquierdo, elija AMI y, a continuación, seleccione la AMI.
3. Compruebe el campo Hora de obsolescencia (si seleccionó la casilla de verificación situada junto a la AMI, se encontrará en la pestaña Detalles). El campo muestra la fecha y la hora de obsolescencia de la AMI. Si el campo está vacío, la AMI no ha quedado obsoleta.

Para filtrar las AMI por la fecha de baja

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación izquierdo, elija AMIs (AMI).
3. En la barra de filtros, elija De mi propiedad o Imágenes privadas (las imágenes privadas incluyen tanto las AMI que se comparten con usted como las que le pertenecen).
4. En la barra de búsqueda, escriba **`Deprecation time`** (al ingresar las letras, aparecerá el filtro Hora de obsolescencia). A continuación, elija un operador y una fecha y una hora.

AWS CLI

Cuando se describen todas las AMI con el comando describe-images, los resultados difieren en función de si usted es un usuario de AMI o el propietario de la AMI.

- Si usted es un usuario de AMI:

  De forma predeterminada, cuando se describen todas las AMI con el comando describe-images, las AMI obsoletas que no son propiedad suya, pero que se comparten con usted, no aparecen en los resultados. Esto se debe a que el valor predeterminado es `--no-include-deprecated`. Para incluir AMI obsoletas en los resultados, debe especificar el parámetro `--include-deprecated`.
- Si usted es el propietario de la AMI:

  Cuando se describen todas las AMI mediante el comando describe-images, todas las AMI que posee, incluidas las AMI obsoletas, aparecen en los resultados. No es necesario especificar el parámetro `--include-deprecated`. Además, no puede excluir de los resultados las AMI obsoletas que posee mediante `--no-include-deprecated`.

Si una AMI está obsoleta, el campo `DeprecationTime` aparece en los resultados.

> **Note**
>
> Una AMI obsoleta es una AMI con fecha de baja en el pasado. Si ha establecido una fecha de baja futura, la AMI aún no se dará de baja.

Para incluir todas las AMI dadas de baja cuando se detallen todas las AMI

Use el comando describe-images y especifique el parámetro `--include-deprecated` para incluir en los resultados todas las AMI obsoletas que no son de su propiedad.

```
aws ec2 describe-images \
    --region us-east-1 \
    --owners 123456example
    --include-deprecated
```

Para detallar la fecha de baja de una AMI

Utilice el comando describe-images y especifique el ID de la AMI.

Tenga en cuenta que si especifica `--no-include-deprecated` junto con el ID de AMI, la AMI obsoleta volverá a aparecer en los resultados.

```
aws ec2 describe-images \
```

```
    --region us-east-1 \
    --image-ids ami-1234567890EXAMPLE
```

Salida prevista

El campo `DeprecationTime` muestra la fecha en la que la AMI está configurada para ser dada de baja. Si la AMI no está configurada para ser dada de baja, el campo `DeprecationTime` no aparecerá en la salida.

```
{
    "Images": [
        {
            "VirtualizationType": "hvm",
            "Description": "Provided by Red Hat, Inc.",
            "PlatformDetails": "Red Hat Enterprise Linux",
            "EnaSupport": true,
            "Hypervisor": "xen",
            "State": "available",
            "SriovNetSupport": "simple",
            "ImageId": "ami-1234567890EXAMPLE",
            "DeprecationTime": "2021-05-10T13:17:12.000Z"
            "UsageOperation": "RunInstances:0010",
            "BlockDeviceMappings": [
                {
                    "DeviceName": "/dev/sda1",
                    "Ebs": {
                        "SnapshotId": "snap-111222333444aaabb",
                        "DeleteOnTermination": true,
                        "VolumeType": "gp2",
                        "VolumeSize": 10,
                        "Encrypted": false
                    }
                }
            ],
            "Architecture": "x86_64",
            "ImageLocation": "123456789012/RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-
GP2",
            "RootDeviceType": "ebs",
            "OwnerId": "123456789012",
            "RootDeviceName": "/dev/sda1",
            "CreationDate": "2019-05-10T13:17:12.000Z",
            "Public": true,
            "ImageType": "machine",
```

```
            "Name": "RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-GP2"
        }
    ]
}
```

Cancelar la baja de una AMI

Puede cancelar la baja de una AMI, lo que eliminará la fecha y la hora del campo Hora de obsolescencia (consola) o del campo `DeprecationTime` de la salida describe-images (AWS CLI). Debe ser el propietario de la AMI para realizar este procedimiento.

Console

Para cancelar la baja de una AMI

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación izquierdo, elija AMI.
3. En la barra de filtros, elija Owned by me (De mi propiedad).
4. Seleccione la AMI y, a continuación, elija Actions (Acciones), Manage AMI Deprecation (Administrar la obsolescencia de la AMI). Puede seleccionar varias AMI para cancelar la baja de varias AMI al mismo tiempo.
5. Desactive la casilla de verificación Habilitar y, luego, elija Guardar.

AWS CLI

Para cancelar la baja de una AMI

Utilice el comando desable-image-deprecation y especifique el ID de la AMI.

```
aws ec2 disable-image-deprecation \
    --image-id ami-1234567890abcdef0
```

Resultado previsto

```
{
  "Return": "true"
}
```

Deshabilitación de una AMI

Puede deshabilitar una AMI para evitar que se utilice en inicializaciones de instancias. No puede iniciar nuevas instancias desde una AMI deshabilitada. Puede volver a habilitar una AMI desactivada para que pueda volver a usarse en inicializaciones de instancias.

> **Warning**
>
> Al deshabilitar una AMI, se eliminan todos sus permisos de inicialización.

Cuando una AMI está deshabilitada:

- El estado de la AMI cambia a `disabled`.
- No se puede compartir una AMI deshabilitada. Si una AMI era pública o se había compartido anteriormente, pasa a ser privada. Si se ha compartido una AMI con una Cuenta de AWS, una organización o unidad organizativa, esta pierde el acceso a la AMI deshabilitada.
- De forma predeterminada, una AMI deshabilitada no aparece en las llamadas a la API DescribeImages.
- Una AMI deshabilitada no aparece en el filtro de la consola De mi propiedad. Para buscar las AMI deshabilitadas, utilice el filtro de la consola Imágenes deshabilitadas.
- Una AMI deshabilitada no está disponible para seleccionarla en inicializaciones de instancias en la consola de EC2. Por ejemplo, una AMI deshabilitada no aparece en el catálogo de AMI en el asistente de inicialización de instancias o al crear una plantilla de inicialización.
- Los servicios de inicialización, como plantillas de inicialización y grupos de escalado automático, pueden seguir haciendo referencia a AMI deshabilitadas. Las inicializaciones posteriores de instancias desde una AMI deshabilitada fallarán, por lo que recomendamos actualizar las plantillas de inicialización y los grupos de escalado automático para que hagan referencia únicamente a las AMI disponibles.
- Las instancias de EC2 que se iniciaron anteriormente mediante una AMI que posteriormente queda deshabilitada no se ven afectadas y pueden detenerse, iniciarse y reiniciarse.
- No puede eliminar las instantáneas asociadas a las AMI deshabilitadas. Si se intenta eliminar una instantánea asociada, se produce el error `snapshot is currently in use`.

Cuando se vuelve a habilitar una AMI:

- El estado de la AMI cambia a `available` y se puede usar para iniciar instancias.
- La AMI se puede compartir.
- Las Cuentas de AWS, las organizaciones y las unidades organizativas que perdieron el acceso a la AMI cuando estaba deshabilitada no recuperan el acceso automáticamente, pero la AMI se puede volver a compartir con ellas.

Puede deshabilitar las AMI privadas y públicas.

Temas

Costos

Cuando se deshabilita una AMI, esta no se elimina. Si la AMI es una AMI respaldada por EBS, seguirá pagando por las instantáneas de EBS de la AMI. Si desea conservar la AMI, es posible que pueda reducir los costos de almacenamiento si archiva las instantáneas. Para obtener más información, consulte Archivar instantáneas de Amazon EBS en la Guía del usuario de Amazon EBS. Si no quiere conservar la AMI y sus instantáneas, debe anular el registro de la AMI y eliminar las instantáneas. Para obtener más información, consulte Eliminar los recursos asociados a su AMI basada en Amazon EBS.

Requisitos previos

Para deshabilitar o volver a habilitar una AMI, debe ser el propietario de la AMI.

Permisos de IAM necesarios

Para deshabilitar y volver a habilitar una AMI, debe tener los siguientes permisos de IAM:

- `ec2:DisableImage`

- `ec2:EnableImage`

Deshabilitación de una AMI

Puede deshabilitar una AMI mediante la consola de EC2 o AWS Command Line Interface (AWS CLI). Debe ser el propietario de la AMI para realizar este procedimiento.

Console

Para deshabilitar una AMI

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación izquierdo, elija AMI.
3. En la barra de filtros, elija De mi propiedad.
4. Seleccione la AMI y, a continuación, elija Acciones, Deshabilitar AMI. Puede seleccionar varias AMI para deshabilitarlas a la vez.
5. En la ventana Deshabilitar AMI, seleccione Deshabilitar AMI.

AWS CLI

Para deshabilitar una AMI

Utilice el comando disable-image y especifique el ID de la AMI.

```
aws ec2 disable-image --image-id ami-1234567890abcdef0
```

Resultado previsto

```
{
  "Return": "true"
}
```

Descripción de las AMI deshabilitadas

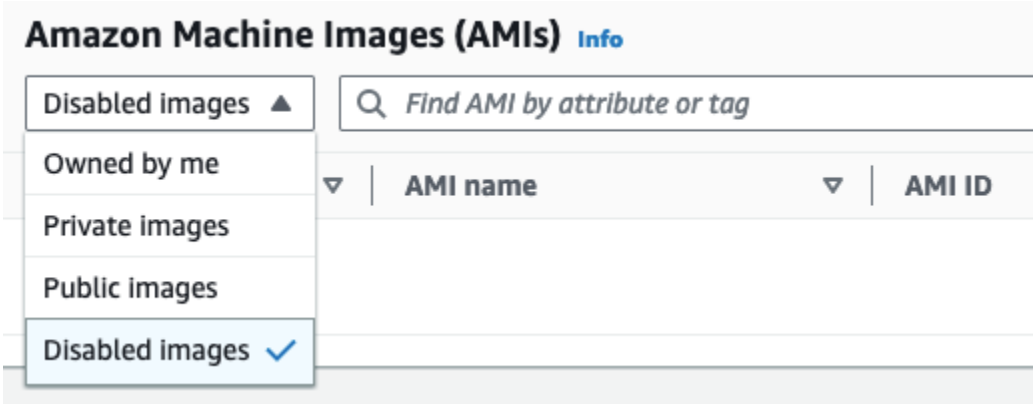
Puede ver las AMI deshabilitadas en la consola de EC2 y mediante AWS CLI.

Debe tener la propiedad de la AMI para ver las AMI deshabilitadas. Como las AMI deshabilitadas se convierten en privadas, no podrá ver las AMI deshabilitadas que no sean de su propiedad.

Console

Para ver las AMI deshabilitadas

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación izquierdo, elija AMI.
3. En la barra de filtros, elija Imágenes deshabilitadas.



AWS CLI

De forma predeterminada, cuando se utiliza el comando describe-images para describir todas las AMI, las AMI deshabilitadas no aparecen en los resultados. Esto se debe a que el valor predeterminado es `--no-include-disabled`. Para incluir AMI deshabilitadas en los resultados, debe especificar el parámetro `--include-disabled`.

Para incluir todas las AMI deshabilitadas cuando se describen todas las AMI

Utilice el comando describe-images y especifique el parámetro `--include-disabled` para recuperar las AMI deshabilitadas, además de todas las demás AMI. Si lo desea, especifique `--owners self` para que solo se recuperen las AMI de su propiedad.

```
aws ec2 describe-images \
    --region us-east-1 \
    --owners self
    --include-disabled
```

Si especifica el ID de una AMI deshabilitada, pero no especifica `--include-disabled`, la AMI deshabilitada aparecerá en los resultados.

```
aws ec2 describe-images \
```

```
    --region us-east-1 \
    --image-ids ami-1234567890EXAMPLE
```

Para recuperar solo las AMI deshabilitadas

Especifique `--filters Name=state,Values=disabled`. También debe especificar `--include-disabled`, de lo contrario obtendrá un error.

```
aws ec2 describe-images \
    --include-disabled \
    --filters Name=state,Values=disabled
```

Ejemplo de resultado

El campo `State` muestra el estado de una AMI. `disabled` indica que la AMI está deshabilitada.

```
{
    "Images": [
        {
            "VirtualizationType": "hvm",
            "Description": "Provided by Red Hat, Inc.",
            "PlatformDetails": "Red Hat Enterprise Linux",
            "EnaSupport": true,
            "Hypervisor": "xen",
            "State": "disabled",
            "SriovNetSupport": "simple",
            "ImageId": "ami-1234567890EXAMPLE",
            "DeprecationTime": "2023-05-10T13:17:12.000Z"
            "UsageOperation": "RunInstances:0010",
            "BlockDeviceMappings": [
                {
                    "DeviceName": "/dev/sda1",
                    "Ebs": {
                        "SnapshotId": "snap-111222333444aaabb",
                        "DeleteOnTermination": true,
                        "VolumeType": "gp2",
                        "VolumeSize": 10,
                        "Encrypted": false
                    }
                }
            ],
            "Architecture": "x86_64",
```

```
            "ImageLocation": "123456789012/RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-
GP2",
            "RootDeviceType": "ebs",
            "OwnerId": "123456789012",
            "RootDeviceName": "/dev/sda1",
            "CreationDate": "2019-05-10T13:17:12.000Z",
            "Public": false,
            "ImageType": "machine",
            "Name": "RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-GP2"
        }
    ]
}
```

Rehabilitación de una AMI deshabilitada

Puede volver a habilitar una AMI deshabilitada. Debe ser el propietario de la AMI para realizar este procedimiento.

Console

Para volver a habilitar una AMI deshabilitada

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación izquierdo, elija AMI.
3. En la barra de filtros, elija Imágenes deshabilitadas.
4. Seleccione la regla y, a continuación, elija Acciones, Habilitar AMI. Puede seleccionar varias AMI para volver a habilitar varias AMI al mismo tiempo.
5. En la ventana Habilitar AMI, seleccione Habilitar.

AWS CLI

Para volver a habilitar una AMI deshabilitada

Utilice el comando enable-image y especifique el ID de la AMI.

```
aws ec2 enable-image --image-id ami-1234567890abcdef0
```

Resultado previsto

```
{
  "Return": "true"
}
```

Archivado de instantáneas de AMI

Puede archivar las instantáneas asociadas a las AMI deshabilitadas respaldadas por EBS. Esto puede ayudarlo a reducir los costos de almacenamiento asociados a las AMI que se utilizan con poca frecuencia y que deben conservarse durante periodos prolongados. Para obtener más información, consulte Archivar instantáneas de Amazon EBS en la Guía del usuario de Amazon EBS.

Para archivar las instantáneas asociadas a una AMI

1. Deshabilite la AMI.
2. Archive las instantáneas.

No puede usar una AMI si está deshabilitada y sus instantáneas asociadas están archivadas.

Para restaurar una AMI deshabilitada con instantáneas archivadas para su uso

1. Restaure las instantáneas archivadas asociadas a la AMI.
2. Habilite la AMI.

Anular el registro de (eliminar) una AMI

Al anular el registro de una AMI, Amazon EC2 la elimina permanentemente. Después de anular el registro de una AMI, no puede utilizarla para iniciar nuevas instancias. Puede anular el registro de una AMI cuando haya terminado de usarla.

Para protegerse de la anulación del registro accidental o malintencionada de una AMI, puede activar la protección contra la anulación de registros. Si anula accidentalmente el registro de una AMI respaldada por EBS, puede utilizar la papelera de reciclaje para restaurarla solo si la restaura dentro del periodo permitido antes de que se elimine de forma permanente.

Mediante la anulación del registro de una AMI no se afectan las instancias que se iniciaron desde dicha AMI. Puede seguir utilizando estas instancias. La anulación del registro de una AMI tampoco afecta las instantáneas que se hayan creado durante el proceso de creación de la AMI. Siguen

sujetos a cobro los costos de uso de esas instancias y los costos de almacenamiento de las instantáneas. Por lo tanto, para evitar incurrir en costos innecesarios, le recomendamos que cierre las instancias y elimine las instantáneas que no necesite. Para obtener más información, consulte Evite los costos derivados de los recursos no utilizados.

Contenido

Consideraciones

- No puede anular el registro de una AMI que no pertenece a su cuenta.
- No puede anular el registro de una AMI administrada por el servicio AWS Backup con Amazon EC2. En su lugar, utilice AWS Backup para eliminar los puntos de recuperación correspondientes en el almacén de copia de seguridad. Para obtener más información, consulte Eliminación de copias de seguridad en la Guía para desarrolladores de AWS Backup.

Anulación del registro de una AMI

Utilice cualquiera de los siguientes métodos para anular el registro de una AMI respaldada por EBS o por el almacén de instancias.

> **Tip**
>
> Para evitar incurrir en costos innecesarios, debe eliminar los recursos que no necesite. Por ejemplo, en el caso de las AMI respaldadas por EBS, si no necesita las instantáneas asociadas a la AMI anulada, debe eliminarlas. Para obtener más información, consulte Evite los costos derivados de los recursos no utilizados.

Console

Para anular el registro de una AMI

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione AMIs.
3. En la barra de filtros, seleccione Propios para ver las AMI disponibles o Imágenes deshabilitadas para ver las AMI deshabilitadas.
4. Seleccione la AMI para anular el registro.
5. Elija Acciones, Anular registro de AMI.
6. Cuando reciba la solicitud de confirmación, elija Anular registro de AMI.

   La consola puede tardar unos minutos en quitar la AMI de la lista. Elija Refresh (Actualizar) para actualizar el estado.

AWS CLI

Para anular el registro de una AMI

Utilice el comando deregister-image y especifique el ID de la AMI cuyo registro desea anular.

```
aws ec2 deregister-image --image-id ami-0123456789example
```

Powershell

Para anular el registro de una AMI

Utilice el cmdlet Unregister-EC2Image y especifique el ID de la AMI cuyo registro desea anular.

```
Unregister-EC2Image -ImageId ami-0123456789example
```

Compruebe cuándo se utilizó una AMI por última vez

`LastLaunchedTime` es una marca de tiempo que indica cuándo se utilizó la AMI por última vez para iniciar una instancia. Las AMI que no se hayan utilizado recientemente para iniciar una instancia pueden ser buenas opciones para darlas de baja o anular su registro.

> **Note**
>
> - Cuando se utiliza la AMI para iniciar una instancia, hay una demora de 24 horas antes de que se informe del uso.
> - Los datos de `lastLaunchedTime` están disponibles a partir de abril de 2017.

Console

Para ver el momento de la última inicialización de una AMI

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación izquierdo, elija AMI.
3. En la barra de filtros, elija De mi propiedad.
4. Seleccione la AMI, y luego compruebe el campo Momento de la última inicialización (si ha seleccionado la casilla de verificación situada junto a la AMI, se encuentra en la pestaña Detalles. El campo muestra la fecha y la hora en que se utilizó la AMI por última vez para iniciar una instancia.

AWS CLI

Puede usar el comando describe-images o describe-image-attribute para ver la última hora en que se inició una AMI.

Para ver la hora del último lanzamiento de una AMI mediante el uso de describe-images

Utilice el comando describe-images y especifique el ID de la AMI.

```
aws ec2 describe-images --image-id ami-0123456789example
```

Ejemplo de resultado

> **Note**
>
> El campo `LastLaunchedTime` solo aparece en la salida de las AMI de su propiedad.

```
{
```

```
    "Images": [
       {
           ...
           "LastLaunchedTime": {
               "Value": "2024-04-02T02:03:18Z"
           },
           ...
       }
   ]
}
```

Para ver el momento de la última inicialización de una AMI

Ejecute el comando describe-image-attribute y especifique `--attribute lastLaunchedTime`. Debe ser el propietario de la AMI para ejecutar este comando.

```
aws ec2 describe-image-attribute \
    --image-id ami-0123456789example \
    --attribute lastLaunchedTime
```

Ejemplo de resultado

```
{
    "ImageId": "ami-1234567890example",
    "LastLaunchedTime": {
        "Value": "2022-02-10T02:03:18Z"
    }
}
```

Proteja una AMI de la anulación del registro

Puede activar la protección contra la anulación del registro en una AMI para evitar su eliminación accidental o malintencionada. Cuando se activa la protección contra la anulación del registro, ningún usuario puede anular el registro de la AMI, independientemente de sus permisos de IAM. Si desea anular el registro de la AMI, primero debe desactivar la protección de anulación del registro que contiene.

Al activar la protección contra la anulación del registro en una AMI, tiene la opción de incluir un periodo de recuperación de 24 horas. Este periodo de recuperación es el tiempo durante el cual la protección por anulación del registro permanece en vigor después de desactivarla. Durante este

periodo de recuperación, no se puede anular el registro de la AMI. Cuando finaliza el periodo de recuperación, se puede anular el registro de la AMI.

La protección contra la anulación del registro está desactivada de forma predeterminada en todas las AMI nuevas y existentes.

Activar la protección contra la anulación del registro

Utilice cualquiera de los siguientes métodos para activar la protección contra la anulación del registro en una AMI. Para ello, debe ser el propietario de la AMI.

Console

Para activar la protección contra la anulación del registro en una AMI

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione AMIs.
3. En la barra de filtros, seleccione Propios para ver las AMI disponibles o Imágenes deshabilitadas para ver las AMI deshabilitadas.
4. Seleccione la AMI en la que desee activar la protección contra la anulación del registro y, a continuación, elija Acciones, Administrar la protección contra la anulación del registro de la AMI.
5. En el cuadro de diálogo Administrar la protección contra la anulación del registro de la AMI, puede activar la protección contra la anulación del registro con o sin un periodo de recuperación. Seleccione una de las siguientes opciones:
   - Activar con un periodo de recuperación de 24 horas: con un periodo de recuperación, no se puede anular el registro de la AMI durante 24 horas si la protección contra la anulación del registro está desactivada.
   - Activar sin periodo de recuperación: sin un periodo de recuperación, se puede anular el registro de la AMI inmediatamente cuando se desactiva la protección contra la anulación del registro.
6. Seleccione Guardar.

AWS CLI

Para activar la protección contra la anulación del registro en una AMI

Utilice el comando enable-image-deregistration-protection y especifique el ID de la AMI. Para incluir el periodo de recuperación opcional de 24 horas, configure `--with-cooldown` en `true`. Para excluir el periodo de recuperación, omita el parámetro `--with-cooldown`.

```
aws ec2 enable-image-deregistration-protection \
    --image-id ami-0123456789example \
    --with-cooldown true
```

Desactivar la protección contra la anulación del registro

Utilice cualquiera de los siguientes métodos para desactivar la protección contra la protección del registro en una AMI. Para ello, debe ser el propietario de la AMI.

> **Note**
>
> Si optó por incluir un periodo de recuperación de 24 horas al activar la protección contra la anulación del registro de la AMI, al desactivar dicha protección no podrá anular inmediatamente el registro de la AMI. El periodo de recuperación es el periodo de 24 horas durante el cual la protección contra la anulación del registro permanece en vigor incluso después de desactivarla. Durante este periodo de recuperación, no se puede anular el registro de la AMI. Cuando finaliza el periodo de recuperación, se puede anular el registro de la AMI.

Console

Para desactivar la protección contra la anulación del registro en una AMI

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione AMIs.
3. En la barra de filtros, seleccione Propios para ver las AMI disponibles o Imágenes deshabilitadas para ver las AMI deshabilitadas.
4. Seleccione la AMI para desactivar la protección contra la anulación del registro y, a continuación, elija Acciones, Administrar la protección contra la anulación del registro de la AMI.
5. En el cuadro de diálogo Administrar la protección contra la anulación del registro de la AMI, seleccione Deshabilitar.

6. Seleccione Guardar.

AWS CLI

Para desactivar la protección contra la anulación del registro en una AMI

Utilice el comando desable-image-deregistration-protection y especifique el ID de la AMI.

```
aws ec2 disable-image-deregistration-protection --image-id ami-0123456789example
```

Evite los costos derivados de los recursos no utilizados

Cuando se anula el registro de una AMI, no se eliminan los recursos que están asociados a dicha AMI. Estos recursos incluyen las instantáneas de las AMI basadas en EBS y los archivos en Amazon S3 para AMI basadas en el almacén de instancias. Cuando se anula el registro de una AMI, tampoco se finalizan ni detienen las instancias iniciadas desde dicha AMI.

Seguirá incurriendo en costos por el almacenamiento de las instantáneas y los archivos, así como por cualquier instancia en ejecución. Para obtener más información, consulte Cómo se cobra.

Para evitar este tipo de costos innecesarios, le recomendamos que elimine los recursos que no necesite.

Para determinar si la AMI está basada en EBS o en el almacén de instancias, consulte Determinar el tipo de dispositivo raíz de su AMI.

Eliminar los recursos asociados a su AMI basada en Amazon EBS

Utilice cualquiera de los siguientes métodos para eliminar los recursos asociados a la AMI basada en EBS.

Console

Para eliminar los recursos asociados a la AMI basada en EBS

1. Anule el registro de la AMI.

   Tome nota del ID de la AMI: esto puede ayudar a encontrar las instantáneas que se eliminarán en el siguiente paso.

2. Elimine todas las instantáneas que no necesite.

   El ID de la AMI asociada se muestra en la columna Descripción de la pantalla de instantáneas.

3. Finalice las instancias que no necesite.

AWS CLI

Para eliminar los recursos asociados a la AMI basada en EBS

1. Anule el registro de la AMI mediante el comando deregister-image.

```
aws ec2 deregister-image --image-id ami-0123456789example
```

2. Elimine las instantáneas que ya no son necesarias mediante el comando delete-snapshot.

```
aws ec2 delete-snapshot --snapshot-id snap-0123456789example
```

3. Finalice las instancias que no necesite mediante el comando terminate-instances.

```
aws ec2 terminate-instances --instance-ids i-0123456789example
```

PowerShell

Para eliminar los recursos asociados a la AMI basada en EBS

1. Anule el registro de la AMI mediante el cmdlet Unregister-EC2Image.

```
Unregister-EC2Image -ImageId ami-0123456789example
```

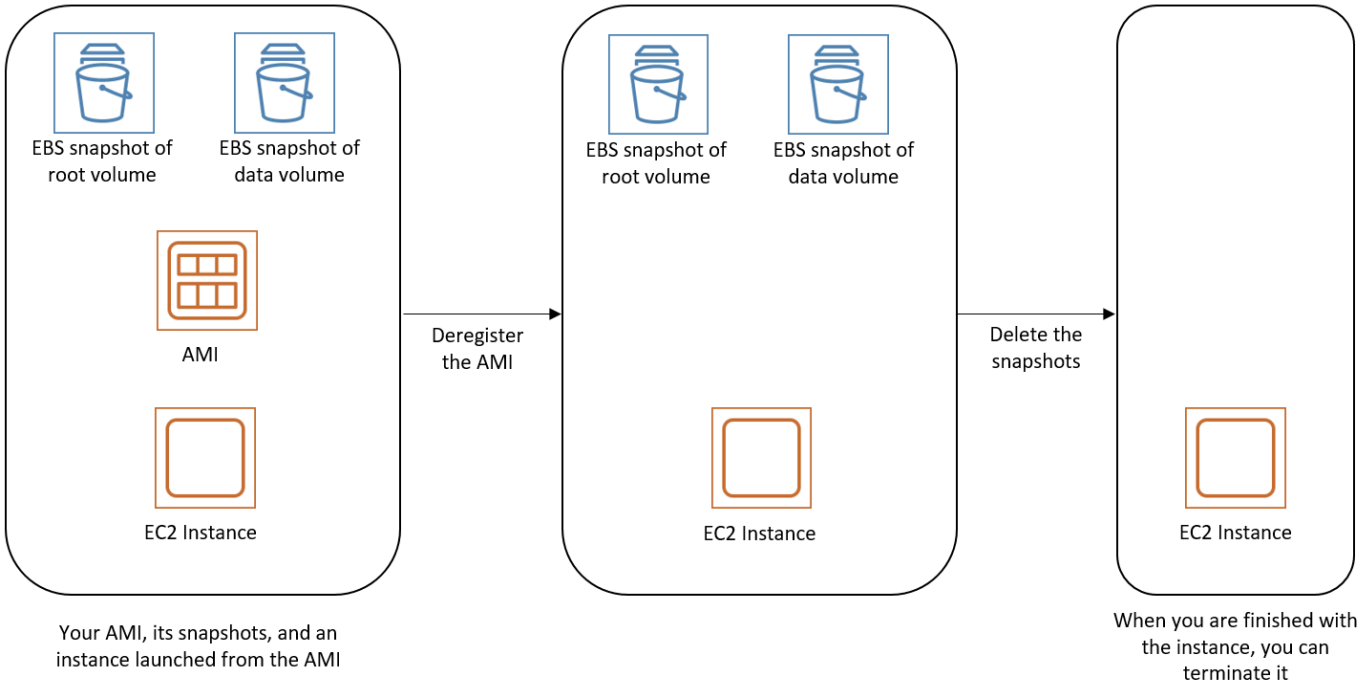
2. Elimine las instantáneas que ya no necesite mediante el cmdlet Remove-EC2Snapshot.

```
Remove-EC2Snapshot -SnapshotId snap-0123456789example
```

3. Finalice las instancias que no necesite mediante el cmdlet Remove-EC2Instance.

```
Remove-EC2Instance -InstanceId i-0123456789example
```

En el siguiente diagrama, se ilustra el flujo de eliminación de los recursos asociados a una AMI basada en EBS.



Eliminar los recursos asociados a la AMI basada en el almacén de instancias

Utilice el siguiente método para eliminar los recursos asociados a la AMI basada en el almacén de instancias.

Para eliminar los recursos asociados a la AMI basada en el almacén de instancias

1. Anule el registro de la AMI mediante el comando deregister-image.

```
aws ec2 deregister-image --image-id ami-0123456789example
```

2. Elimine el paquete en Amazon S3 con el comando ec2-delete-bundle (herramientas de la AMI).

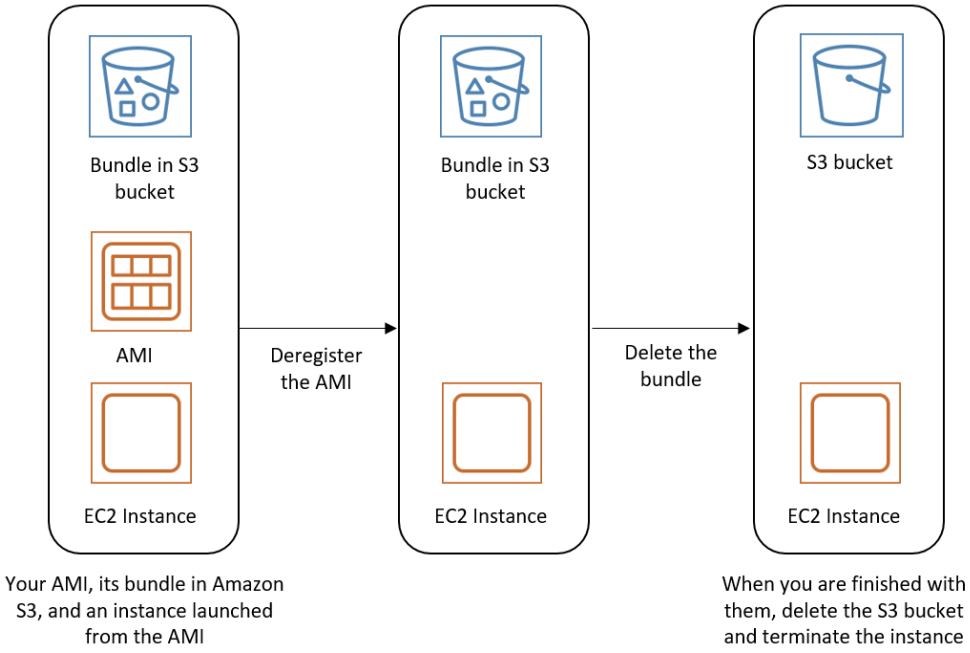
```
ec2-delete-bundle -b myawsbucket/myami -a your_access_key_id -
s your_secret_access_key -p image
```

3. Finalice las instancias que no necesite mediante el comando terminate-instances.

```
aws ec2 terminate-instances --instance-ids i-0123456789example
```

4. Si ya no utiliza el bucket de Amazon S3 en el que cargó el paquete, puede eliminarlo. Para eliminar un bucket de Amazon S3, abra la consola de Amazon S3 seleccione el bucket, elija Acciones y, a continuación, elija Eliminar.

En el siguiente diagrama, se ilustra el flujo de eliminación de los recursos asociados a la AMI basada en el almacén de instancias.



Automatizar el ciclo de vida de la AMI con respaldo en EBS

Puede utilizar Amazon Data Lifecycle Manager para automatizar la creación, retención, copia, obsolescencia y cancelación del registro de las AMI basadas en Amazon EBS y sus instantáneas de respaldo. Para obtener más información, consulte Amazon Data Lifecycle Manager.

Usar el cifrado con las AMI con respaldo de EBS

Las AMI que cuentan con el respaldo de instantáneas de Amazon EBS pueden beneficiarse del cifrado Amazon EBS. Las instantáneas de datos y volúmenes raíz se pueden cifrar y adjuntar a una AMI. Puede iniciar instancias y copiar imágenes con el soporte para el cifrado EBS completo incluido. Los parámetros de cifrado para estas operaciones se admiten en todas las regiones donde AWS KMS está disponible.

Las instancias de EC2 con volúmenes de EBS cifrados se inician desde las AMIs de la misma forma que otras instancias. Además, cuando lance una instancia desde una AMI respaldada por instantáneas EBS sin cifrar, puede cifrar algunos o todos los volúmenes durante la inicialización.

Al igual que los volúmenes de EBS, las instantáneas de las AMI se pueden cifrar de forma predeterminada mediante la AWS KMS key o a una clave administrada por el cliente que especifique. En todos los casos, debe tener permiso para usar la Clave de KMS seleccionada.

Las AMI con instantáneas cifradas se pueden compartir en cuentas de AWS. Para obtener más información, consulte AMI compartidas.

Temas sobre cifrado con AMI con respaldo de EBS

- Situaciones de inicialización de instancias
- Situaciones de copia de imagen

Situaciones de inicialización de instancias

Las instancias de Amazon EC2 se inician desde las AMI mediante la acción `RunInstances` con los parámetros proporcionados a través de la asignación de dispositivos de bloques, ya sea a través de la AWS Management Console o directamente mediante la API o la CLI de Amazon EC2. Para obtener más información, consulte Mapeos de dispositivos de bloques. Para obtener ejemplos del control de la asignación de dispositivos de bloqueo desde la AWS CLI, consulte inicialización, enumeración y terminación de instancias de EC2.

De forma predeterminada, sin parámetros de cifrado explícitos, una acción `RunInstances` mantiene el estado de cifrado existente de las instantáneas de origen de una AMI mientras que restaura sus volúmenes de EBS. Si se habilita el cifrado de forma predeterminada, todos los volúmenes creados desde la AMI (de instantáneas cifradas o sin cifrar) se cifrarán. Si el cifrado de forma predeterminada no está habilitado, la instancia mantiene el estado de cifrado de la AMI.

También puede iniciar una instancia y solicitar de forma simultánea un nuevo estado de cifrado para los volúmenes restantes al suministrar parámetros de cifrado. Por lo tanto, se observan los siguientes comportamientos:

iniciar sin parámetros de cifrado

- Una instantánea sin cifrar se restaura en un volumen sin cifrar, a menos que se habilite el cifrado de forma predeterminada, en cuyo caso se cifrarán todos los volúmenes recién creados.

- Una instantánea cifrada que usted posee se restaura en un volumen que está cifrado en la misma Clave de KMS.
- Una instantánea cifrada de la que no es propietario (por ejemplo, la AMI se comparte con usted) se restaura en un volumen que está cifrado por la clave de KMS predeterminada de su cuenta de AWS.

Se pueden anular los comportamientos predeterminados al suministrar los parámetros de cifrado. Los parámetros disponibles son `Encrypted` y `KmsKeyId`. Establecimiento de solo los resultados del parámetro `Encrypted` en lo siguiente:

Comportamientos de inicialización de instancia con **`Encrypted`** establecido pero **`KmsKeyId`** sin especificar.

- Una instantánea no cifrada se restaura en un volumen de EBS cifrado por la clave de KMS predeterminada de su cuenta de AWS.
- Una instantánea cifrada que usted posee se restaura en un volumen de EBS cifrado con la misma Clave de KMS. (En otras palabras, el parámetro `Encrypted` no tiene efecto).
- Una instantánea cifrada de la que no es propietario (es decir, la AMI se comparte con usted) se restaura en un volumen que está cifrado por la clave de KMS predeterminada de su cuenta de AWS. (En otras palabras, el parámetro `Encrypted` no tiene efecto).

Establecer los parámetros `KmsKeyId` y `Encrypted` permite especificar una Clave de KMS no predeterminada para una operación de cifrado. Se producen los siguientes comportamientos:

La instancia con **`Encrypted`** y **`KmsKeyId`** establecidos

- Una instantánea no cifrada se restaura en un volumen de EBS cifrado por la Clave de KMS especificada.
- Una instantánea cifrada se restaura en un volumen de EBS cifrado no en la Clave de KMS original, sino en la Clave de KMS especificada.

El envío de un parámetro `KmsKeyId` sin establecer también el parámetro `Encrypted` da como resultado un error.

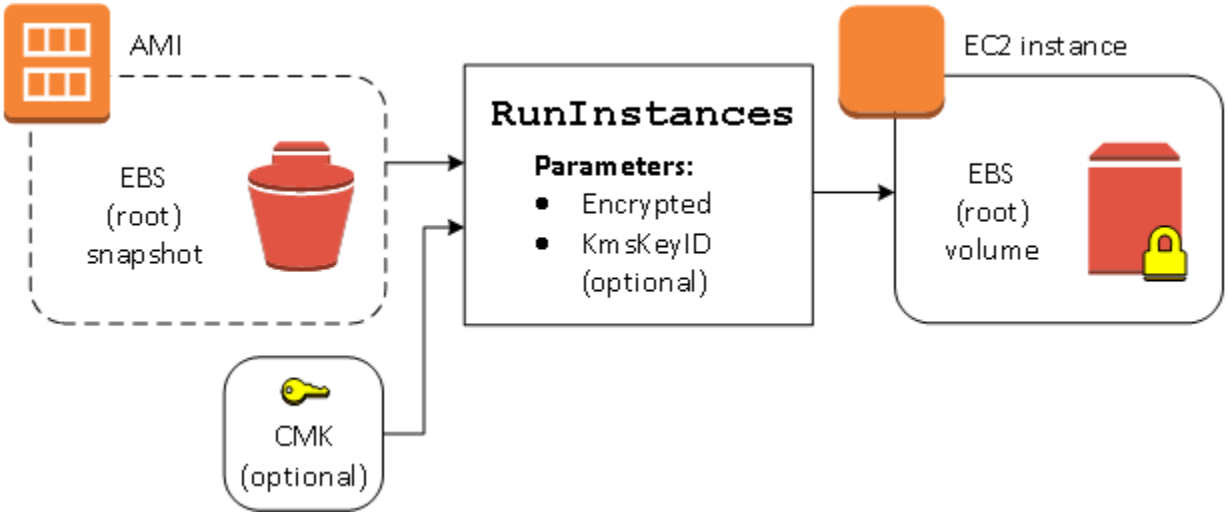
Las siguientes secciones ofrecen ejemplos de inicialización de instancias desde AMI con parámetros de cifrado no predeterminados. En cada una de estas situaciones, los parámetros suministrados

para la acción `RunInstances` da como resultado un cambio en el estado de cifrado durante la restauración de un volumen desde una instantánea.

Para obtener información sobre el uso de la consola para iniciar una instancia desde una AMI, consulte iniciar la instancia.

Cifrar un volumen durante la inicialización

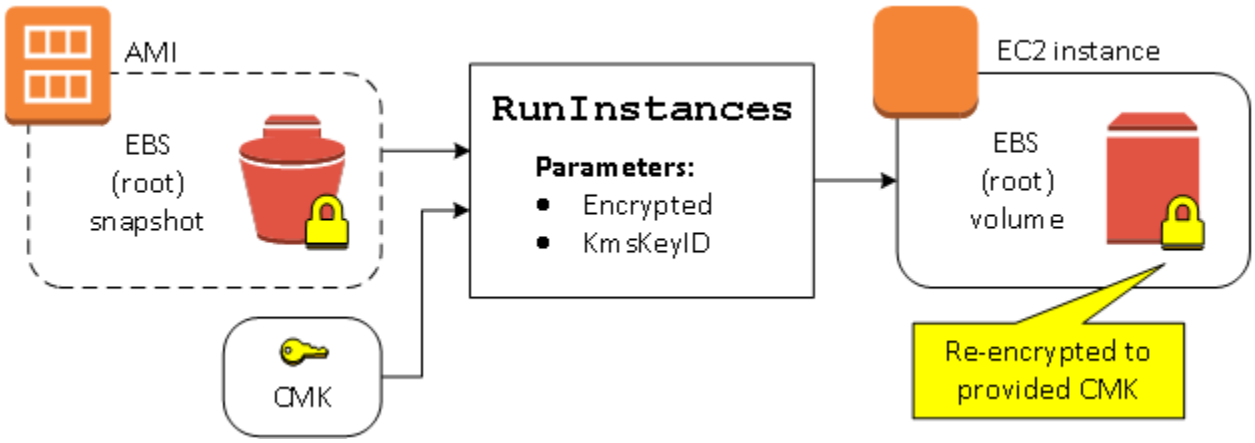
En este ejemplo, una AMI respaldada por una instantánea sin cifrar se utiliza para iniciar una instancia de EC2 con un volumen de EBS cifrado.



El parámetro `Encrypted` por sí solo genera el volumen para esta instancia que se va a cifrar. Proporcionar un parámetro `KmsKeyId` es opcional. Si no se especifica ningún ID de clave de KMS, se utiliza la clave de KMS predeterminada de la cuenta de AWS para cifrar el volumen. Para cifrar el volumen en otra Clave de KMS que usted posee, proporcione el parámetro `KmsKeyId`.

Volver a cifrar un volumen durante la inicialización

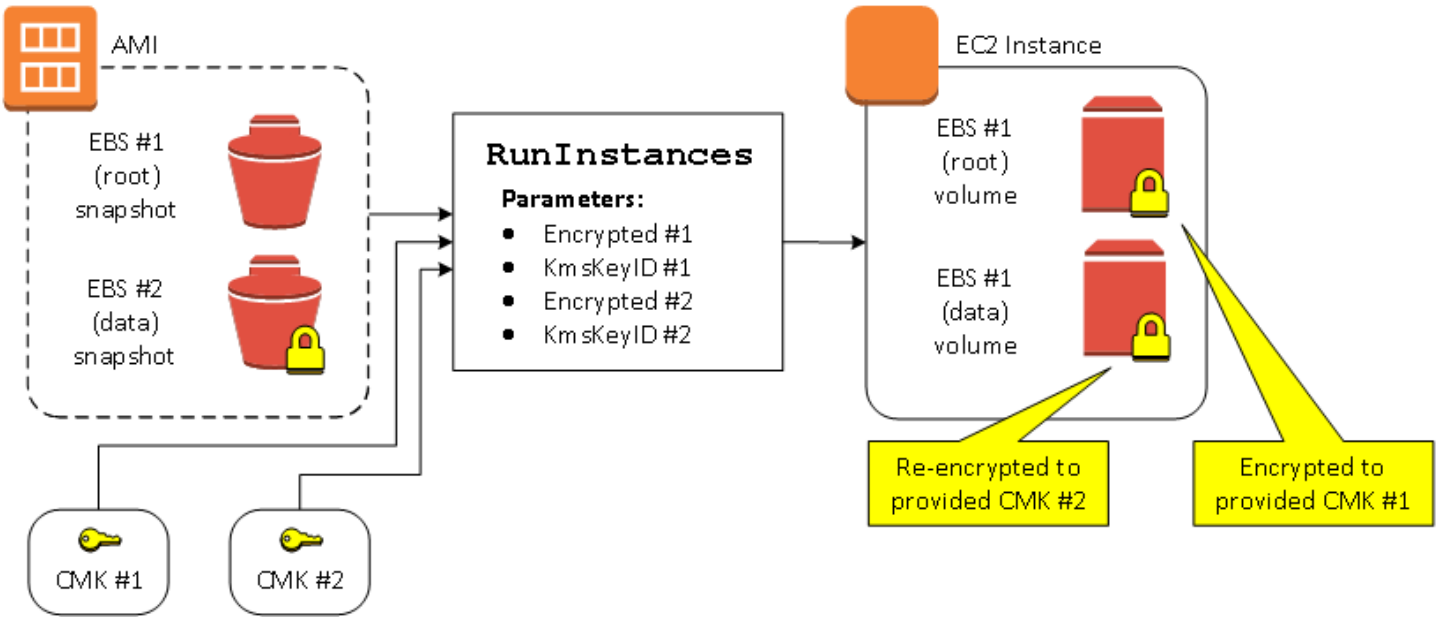
En este ejemplo, una AMI con el respaldo de una instantánea cifrada se utiliza para iniciar una instancia de EC2 con un volumen EBS cifrado por una nueva Clave de KMS.



Si usted es propietario de la AMI y no proporciona parámetros de cifrado, la instancia resultante tiene un volumen cifrado con la misma clave de KMS que la instantánea. Si la AMI se comparte en lugar de ser de su propiedad y no proporciona parámetros de cifrado, el volumen se cifra mediante la Clave de KMS predeterminada. Con los parámetros de cifrado proporcionados como se muestra, el volumen se cifra mediante la Clave de KMS especificada.

Cambiar el estado de cifrado de varios volúmenes durante la inicialización

En este ejemplo más completo, una AMI respaldada por varias instantáneas (cada una con su propio estado de cifrado) se utiliza para iniciar una instancia de EC2 con un volumen recientemente cifrado y un volumen que se ha vuelto a cifrar.



En esta situación, la acción `RunInstances` se suministra con parámetros de cifrado para cada una de las instantáneas del origen. Cuando se especifican todos los parámetros de cifrado posibles, la instancia resultante es la misma sin importar si posee la AMI.

Situaciones de copia de imagen

Las AMI de Amazon EC2 se copian con la acción `CopyImage`, mediante la AWS Management Console o directamente con la API o la CLI de Amazon EC2.

De forma predeterminada, sin parámetros de cifrado explícitos, una acción `CopyImage` mantiene el estado de cifrado existente de las instantáneas de origen de una AMI. También puede copiar una AMI y solicitar de forma simultánea un nuevo estado de en las instantáneas de EBS asociadas al suministrar parámetros de cifrado. Por lo tanto, se observan los siguientes comportamientos:

Copiar sin parámetros de cifrado

- Una instantánea sin cifrar se copia en otra instantánea sin cifrar, a menos que se habilite el cifrado de forma predeterminada, en cuyo caso se cifrarán todos las instantáneas recién creadas.
- Una instantánea cifrada que usted posee se copia en una instantánea cifrada con la misma Clave de KMS.
- Una instantánea cifrada de la que no es propietario (es decir, la AMI se comparte con usted) se copia en una instantánea que está cifrada por la clave de KMS predeterminada de su cuenta de AWS.

Se pueden anular todos estos comportamientos predeterminados al suministrar los parámetros de cifrado. Los parámetros disponibles son `Encrypted` y `KmsKeyId`. Establecimiento de solo los resultados del parámetro `Encrypted` en lo siguiente:

Comportamientos de copy-image con **`Encrypted`** establecida pero **`KmsKeyId`** sin especificar.

- Una instantánea no cifrada se copia en una instantánea cifrada mediante la clave de KMS predeterminada de la cuenta de AWS.
- Una instantánea cifrada se copia en una instantánea cifrada con la misma Clave de KMS. (En otras palabras, el parámetro `Encrypted` no tiene efecto).
- Una instantánea cifrada de la que no es propietario (es decir, la AMI se comparte con usted) se copia en un volumen que está cifrado por la clave de KMS predeterminada de su cuenta de AWS. (En otras palabras, el parámetro `Encrypted` no tiene efecto).

Establecer los parámetros `Encrypted` y `KmsKeyId` permite especificar una Clave de KMS administrada por el cliente para una operación de cifrado. Se producen los siguientes comportamientos:

Comportamientos de copi-image con **`Encrypted`** y **`KmsKeyId`** establecidas

- Una instantánea no cifrada se copia en una instantánea cifrada por la Clave de KMS especificada.
- Una instantánea cifrada se copia en una instantánea cifrada no por la Clave de KMS original, sino por la Clave de KMS especificada.

El envío de un parámetro `KmsKeyId` sin establecer también el parámetro `Encrypted` da como resultado un error.

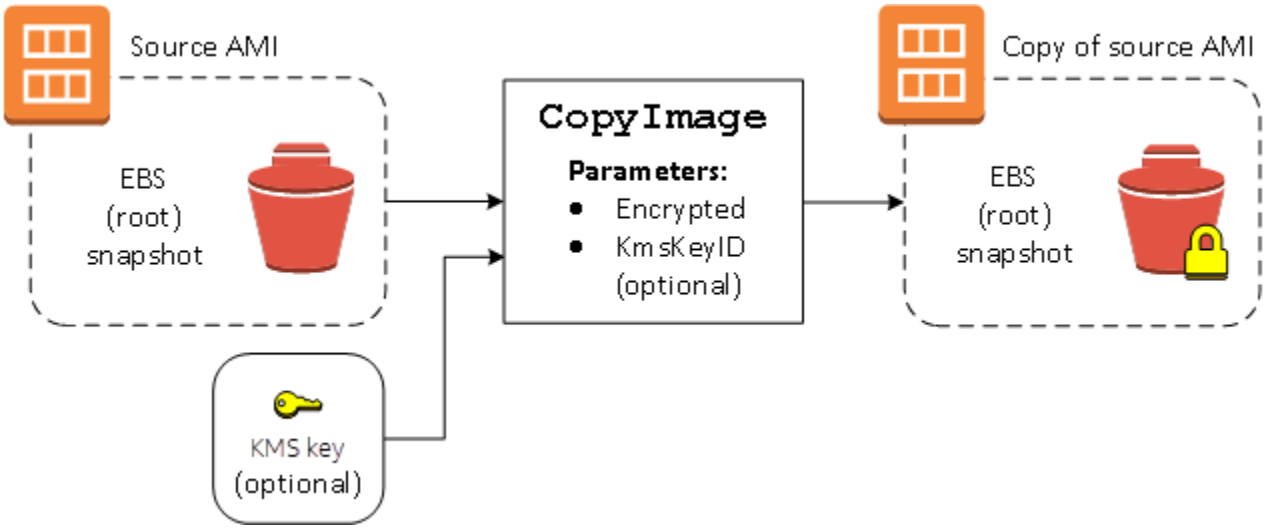
La siguiente sección ofrece un ejemplo de copia de una AMI con parámetros de cifrado no predeterminados, resultantes de un cambio en el estado de cifrado.

Para obtener instrucciones detalladas sobre el uso de la consola, consulte Copiar una AMI.

Cifrar una imagen sin cifrar durante la copia

En este caso, una AMI respaldada por una instantánea raíz no cifrada se copia en una AMI con una instantánea raíz cifrada. La acción `CopyImage` se invoca con dos parámetros de cifrado, incluida una clave administrada por el cliente. Como resultado, el estado de cifrado de la instantánea raíz cambia, de modo que la AMI de destino se respalda por una instantánea raíz que contiene los mismos datos que la instantánea de origen, pero cifrada con la clave especificada. Usted incurre en costos de almacenamiento de las instantáneas en ambas AMI, así como en cargos correspondientes a las instancias que lance desde cualquiera de las AMI.

> **Note**
>
> Habilitar el cifrado de forma predeterminada tiene el mismo efecto que configurar el parámetro `Encrypted` en `true` para todas las instantáneas de la AMI.



La configuración del parámetro `Encrypted` cifra la única instantánea para esta instancia. Si no especifica el parámetro `KmsKeyId`, la clave predeterminada administrada por el cliente se utiliza para cifrar la copia de la instantánea.

> **Note**
>
> También puede copiar una imagen con varias instantáneas y configurar el estado de cifrado de cada una de forma individual.

Supervisión de los eventos de las AMI con Amazon EventBridge

Cuando cambia el estado de una imagen de máquina de Amazon (AMI), Amazon EC2 genera un evento que se envía a Amazon EventBridge (antes conocido como Eventos de Amazon CloudWatch). Puede utilizar Amazon EventBridge para detectar y reaccionar a estos eventos. Para ello, cree reglas en EventBridge que activen una acción como respuesta a un evento. Por ejemplo, puede crear una regla de EventBridge que detecte cuándo se ha completado el proceso de creación de la AMI y, a continuación, invoque un tema de Amazon SNS para que envíe una notificación por email.

Amazon EC2 genera un evento cuando una AMI entra en alguno de los siguientes estados:

- `available`
- `failed`
- `deregistered`

- `disabled`

En la siguiente tabla se enumeran las operaciones de la AMI y los estados que puede adoptar una AMI. En la tabla, Sí indica los estados que la AMI puede adoptar cuando se ejecuta la operación correspondiente.

Operaciones de AMI	available	failed	deregistered	disabled
CopyImage	Sí	Sí		
CreateImage	Sí	Sí		
CreateRestoreImageTask	Sí	Sí		
DeregisterImage			Sí	
DisableImage				Sí
EnableImage	Sí			
RegisterImage	Sí	Sí		

Los eventos se envían en la medida de lo posible.

Temas

- Eventos de la AMI
- Crear reglas de Amazon EventBridge

Eventos de la AMI

Hay cuatro eventos de EC2 AMI State Change:

- available
- failed
- deregistered

- disabled

Los eventos se envían al bus de eventos en EventBridge en formato JSON de manera predeterminada.

Los siguientes campos del evento se pueden utilizar para crear reglas que activen una acción:

`"source": "aws.ec2"`

Identifica que el evento es de Amazon EC2.

`"detail-type": "EC2 AMI State Change"`

Identifica el nombre del evento.

`"detail": { "ImageId": "ami-0123456789example", "State": "available", }`

Proporciona la siguiente información:

- ID de AMI: si desea realizar el seguimiento de una AMI específica.
- El estado de la AMI (`available`, `failed`, `deregistered` o `disabled`).

`available`

A continuación, se muestra un ejemplo de un evento que Amazon EC2 genera cuando la AMI adopta el estado `available` tras una operación `CreateImage`, `CopyImage`, `RegisterImage`, `CreateRestoreImageTask` o `EnableImage` correcta.

`"State": "available"` indica que la operación se ha realizado correctamente.


```
{
    "version": "0",
    "id": "example-9f07-51db-246b-d8b8441bcdf0",
    "detail-type": "EC2 AMI State Change",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1::image/ami-0123456789example"],
    "detail": {
        "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
```

```
        "ImageId": "ami-0123456789example",
        "State": "available",
        "ErrorMessage": ""
    }
}
```

failed

A continuación, se muestra un ejemplo de un evento que Amazon EC2 genera cuando la AMI adopta el estado `failed` tras una operación `CreateImage`, `CopyImage`, `RegisterImage`, `CreateRestoreImageTask` con errores.

En los campos siguientes, se muestra información pertinente:

- `"State": "failed"` indica que se ha producido un error en una operación.
- `"ErrorMessage": ""`: proporciona el motivo de la operación fallida.

```
{
    "version": "0",
    "id": "example-9f07-51db-246b-d8b8441bcdf0",
    "detail-type": "EC2 AMI State Change",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1::image/ami-0123456789example"],
    "detail": {
        "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
        "ImageId": "ami-0123456789example",
        "State": "failed",
        "ErrorMessage": "Description of failure"
    }
}
```

deregistered

A continuación, se muestra un ejemplo de un evento que Amazon EC2 genera cuando la AMI adopta el estado `deregistered` tras una operación `DeregisterImage` correcta. Si la operación falla, no se genera ningún evento. Cualquier error se conoce inmediatamente porque `DeregisterImage` es una operación sincrónica.

`"State": "deregistered"` indica que la operación `DeregisterImage` se ha realizado correctamente.

```
{
    "version": "0",
    "id": "example-9f07-51db-246b-d8b8441bcdf0",
    "detail-type": "EC2 AMI State Change",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1::image/ami-0123456789example"],
    "detail": {
        "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
        "ImageId": "ami-0123456789example",
        "State": "deregistered",
        "ErrorMessage": ""
    }
}
```

`disabled`

A continuación, se muestra un ejemplo de un evento que Amazon EC2 genera cuando la AMI adopta el estado `disabled` tras una operación `DisableImage` correcta. Si la operación falla, no se genera ningún evento. Cualquier error se conoce inmediatamente porque `DisableImage` es una operación sincrónica.

`"State": "disabled"` indica que la operación `DisableImage` se ha realizado correctamente.

```
{
    "version": "0",
    "id": "example-9f07-51db-246b-d8b8441bcdf0",
    "detail-type": "EC2 AMI State Change",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1::image/ami-0123456789example"],
    "detail": {
        "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
        "ImageId": "ami-0123456789example",
        "State": "disabled",
```

```
        "ErrorMessage": ""
    }
}
```

Crear reglas de Amazon EventBridge

Puede crear una Regla de Amazon EventBridge que especifique una acción que se debe realizar cuando EventBridge recibe un evento que coincide con el Patrón de eventos en la regla. Cuando un evento coincide, EventBridge envía el evento al destino especificado y activa la acción definida en la regla.

Los patrones de eventos tienen la misma estructura que los eventos con los que coinciden. Un patrón de evento coincide con un evento o no lo hace.

Cuando crea una regla para un evento de cambio de estado de una AMI, puede incluir los siguientes campos en el patrón de eventos:

`"source": "aws.ec2“`

Identifica que el evento es de Amazon EC2.

`"detail-type": "EC2 AMI State Change"`

Identifica el nombre del evento.

`"detail": { "ImageId": "ami-0123456789example", "State": "available", }`

Proporciona la siguiente información:

- ID de AMI: si desea realizar el seguimiento de una AMI específica.
- El estado de la AMI (`available`, `failed`, `deregistered` o `disabled`).

Ejemplo: creación de una regla de EventBridge para enviar una notificación

En el siguiente ejemplo, se crea una regla de EventBridge para enviar un correo electrónico, un mensaje de texto o una notificación push móvil cuando hay una AMI en estado `available` después de que la operación `CreateImage` se haya completado correctamente.

Antes de crear la regla de EventBridge, debe crear el tema de Amazon SNS para el email, el mensaje de texto o la notificación push móvil.

Para crear una regla de EventBridge para enviar una notificación cuando se crea una AMI y se encuentra en estado **`available`**

1. Abra la consola de Amazon EventBridge en https://console.aws.amazon.com/events/.
2. Elija Crear regla.
3. En Definir detalle de la regla, haga lo siguiente:

   a. Ingrese un Nombre para la regla y, opcionalmente, una descripción.

      Una regla no puede tener el mismo nombre que otra regla de la misma región y del mismo bus de eventos.

   b. En Bus de eventos, elija Predeterminado. Cuando un servicio de AWS en su cuenta emite un evento, siempre se dirige al bus de eventos predeterminado de su cuenta.

   c. En Tipo de regla, elija Regla con un patrón de evento.

   d. Elija Siguiente.

4. En Crear patrón de evento, realice una de las siguientes acciones:

   a. En Origen del evento, elija Eventos o eventos de socios de EventBridge de AWS.

   b. En Event pattern (Patrón de evento), en este ejemplo, especificará el siguiente patrón de evento para que coincida con cualquier evento `EC2 AMI State Change` que se genere cuando una AMI ingresa al estado `available`:

```
{
 "source": ["aws.ec2"],
 "detail-type": ["EC2 AMI State Change"],
 "detail": {"State": ["available"]}
}
```

      Para agregar el patrón de evento, puede utilizar una plantilla por medio de la opción Event pattern form (Formulario de patrón de evento) o puede especificar su propio patrón por medio de la opción Custom pattern (JSON editor) (Patrón personalizado [editor de JSON]), de la siguiente manera:

      i. Para utilizar una plantilla con el objetivo de crear el patrón de evento, haga lo siguiente:

         A. Seleccione Formulario de patrón de evento.

         B. En Origen del evento, elija Servicios de AWS.

C. En Servicio de AWS, elija EC2.

D. En Tipo de evento, elija Cambio de estado de la AMI de EC2.

E. Para personalizar la plantilla, elija Editar patrón y realice los cambios para que coincidan con el patrón de evento de ejemplo.

ii. Para especificar un patrón de evento personalizado, haga lo siguiente:

A. Elija Custom pattern (JSON editor) (Patrón personalizado [editor de JSON]).

B. En el casillero Patrón de evento, agregue el patrón de eventos de este ejemplo.

c. Elija Siguiente.

5. En Seleccionar destino, realice una de las siguientes acciones:

a. En Tipos de destino, elija Servicio de AWS.

b. En Seleccionar un destino, elija Tema de SNS para enviar un email, un mensaje de texto o una notificación push móvil cuando se produzca el evento.

c. En Tema, elija un tema existente. Primero debe crear un tema de Amazon SNS mediante la consola de Amazon SNS. A fin de obtener más información, consulte Uso de Amazon SNS para mensajería de aplicación a persona (A2P) en Guía para desarrolladores de Amazon Simple Notification Service.

d. (Opcional) En Configuración adicional, puede configurar opciones adicionales. Para obtener más información, consulte Creación de reglas de EventBridge que reaccionan a eventos (paso 16) en la Guía del usuario de Amazon EventBridge.

e. Elija Siguiente.

6. (Opcional) En Etiquetas, puede asignar una o varias etiquetas a la regla y, a continuación, elija Siguiente.

7. En Revisar y crear, realice una de las siguientes acciones:

a. Revise los detalles de la regla y modifíquelos según sea necesario.

b. Elija Crear regla.

Para obtener más información, consulte los siguientes temas en la Guía del usuario de Amazon EventBridge:

- Eventos de Amazon EventBridge
- Patrones de eventos Amazon EventBridge

- Reglas de Amazon EventBridge

Para obtener un tutorial sobre cómo crear una función de Lambda y una regla de EventBridge que ejecute la función de Lambda, consulte Tutorial: registrar el estado de una instancia de Amazon EC2 mediante EventBridge en la Guía para desarrolladores de AWS Lambda.

Comprender la información de facturación de la AMI

Hay muchas Imágenes de máquina de Amazon (AMI) entre las que elegir al iniciar las instancias y son compatibles con una variedad de plataformas y características del sistema operativo. Para comprender cómo la AMI que elija cuando lance la instancia afecta los resultados de su factura de AWS, puede investigar la plataforma del sistema operativo asociada y la información de facturación. Haga esto antes de iniciar cualquier instancia bajo demanda o instancias de spot, o antes de comprar una instancia reservada.

Estos son dos ejemplos de cómo puede ayudarlo investigar su AMI con anticipación para elegir la AMI que mejor se adapte a sus necesidades:

- Para instancias de spot, puede utilizar los detalles de la plataforma de la AMI para confirmar que esta es compatible con instancias de spot.
- Al comprar una instancia reservada, puede asegurarse de seleccionar la plataforma del sistema operativo (Plataforma) que se asigna a los detalles de la plataforma de la AMI.

Para obtener más información acerca de los precios de las instancias, consulte Precios de Amazon EC2.

Contenido

Campos de información de facturación de las AMI

Los siguientes campos proporcionan información de facturación asociada a una AMI:

Detalles de la plataforma

Los detalles de la plataforma asociados con el código de facturación de la AMI. Por ejemplo, `Red Hat Enterprise Linux`.

Operación de uso

El funcionamiento de la instancia de Amazon EC2 y el código de facturación asociado a la AMI. Por ejemplo, `RunInstances:0010`. La operación de uso se corresponde con el contenido de la columna lineitem/Operation de su AWS Informe de uso y costo (CUR) y de la API de lista de precios de AWS.

Puede ver estos campos en la página instancias o AMI en la consola de Amazon EC2, o en la respuesta que devuelve el comando describe-images o Get-EC2Image.

Datos de ejemplo: operación de uso por plataforma

La siguiente tabla enumera algunos de los detalles de la plataforma y los valores de operación de uso que se pueden mostrar en las páginas instancias o AMI en la consola de Amazon EC2, o en la respuesta que devuelve el comando describe-images o Get-EC2Image.

Detalles de la plataforma	Operación de uso [2]
Linux/UNIX	RunInstances
Red Hat BYOL Linux	RunInstances:00g0 [3]
Red Hat Enterprise Linux	RunInstances:0010
Red Hat Enterprise Linux with HA	RunInstances:1010
Red Hat Enterprise Linux with SQL Server Standard and HA	RunInstances:1014
Red Hat Enterprise Linux with SQL Server Enterprise and HA	RunInstances:1110
Red Hat Enterprise Linux with SQL Server Standard	RunInstances:0014

Detalles de la plataforma	Operación de uso [2]
Red Hat Enterprise Linux with SQL Server Web	RunInstances:0210
Red Hat Enterprise Linux with SQL Server Enterprise	RunInstances:0110
SQL Server Enterprise	RunInstances:0100
SQL Server Standard	RunInstances:0004
SQL Server Web	RunInstances:0200
SUSE Linux	RunInstances:000g
Ubuntu Pro	RunInstances:0g00
Windows	RunInstances:0002
Windows BYOL	RunInstances:0800
Windows with SQL Server Enterprise [1]	RunInstances:0102
Windows with SQL Server Standard [1]	RunInstances:0006
Windows with SQL Server Web [1]	RunInstances:0202

[1] Si hay dos licencias de software asociadas a una AMI, el campo Detalles de la plataforma muestra ambas.

[2] Si está ejecutando instancias de spot, el lineitem/Operation que aparece en su Informe de costos y uso de AWS puede ser diferente del valor de la operación de uso que aparece aquí. Por ejemplo, si `lineitem/Operation` muestra `RunInstances:0010:SV006`, significa que Amazon EC2 está

ejecutando una instancia de spot Red Hat Enterprise Linux por horas en el Este de EE. UU. (Norte de Virginia) en la Zona 6.

[3] Aparece como RunInstances (Linux/UNIX) en sus informes de uso.

Encontrar detalles de facturación y uso de la AMI

En la consola de Amazon EC2, puede ver la información de facturación de la AMI desde la página AMI o desde la página Instancias. También puede encontrar información de facturación utilizando AWS CLI o el servicio de metadatos de instancia.

Los siguientes campos pueden ayudarlo a verificar los cargos de la AMI en su factura:

- Detalles de la plataforma
- Operación de uso
- ID DE AMI

Encontrar información de facturación de la AMI (consola)

Siga estos pasos para ver la información de facturación de la AMI en la consola de Amazon EC2:

Buscar información de facturación de la AMI en la página AMI

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija AMI y, a continuación, seleccione una AMI.
3. En la ficha Detalles compruebe los valores de Detalles de la plataforma y Operación de uso.

Buscar información de facturación de la AMI en la página Instancias

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instancias y, a continuación, seleccione una instancia.
3. En la ficha Detalles (o en la ficha Descripción si utiliza la versión anterior de la consola), compruebe los valores de Detalles de la plataforma y Operación de uso.

Encontrar información de facturación de la AMI (AWS CLI)

Para encontrar la información de facturación de la AMI utilizando el AWS CLI, necesita conocer el ID de AMI. Si no conoce el ID de AMI, puede obtenerlo de la instancia mediante el comando describe-instances.

Para buscar el ID de AMI

Si conoce el ID de instancia, puede obtener el ID de AMI de la instancia mediante el comando describe-instances.

```
aws ec2 describe-instances --instance-ids i-123456789abcde123
```

En la salida, el ID de AMI se especifica en el campo `ImageId`.

```
..."Instances": [
{
    "AmiLaunchIndex": 0,
    "ImageId": "ami-0123456789EXAMPLE",
    "InstanceId": "i-123456789abcde123",
    ...
}]
```

Para buscar la información de facturación de la AMI

Si conoce el ID de AMI, puede utilizar el comando describe-images para obtener la plataforma de la AMI y los detalles de la operación de uso.

```
$ aws ec2 describe-images --image-ids ami-0123456789EXAMPLE
```

El siguiente resultado de ejemplo muestra los campos `UsageOperation` y `PlatformDetails`. En este ejemplo, la plataforma ami-0123456789EXAMPLE es `Red Hat Enterprise Linux` y la operación de uso y el código de facturación son `RunInstances:0010`.

```
{
    "Images": [
        {
            "VirtualizationType": "hvm",
            "Description": "Provided by Red Hat, Inc.",
            "Hypervisor": "xen",
```

```
            "EnaSupport": true,
            "SriovNetSupport": "simple",
            "ImageId": "ami-0123456789EXAMPLE",
            "State": "available",
            "BlockDeviceMappings": [
                {
                    "DeviceName": "/dev/sda1",
                    "Ebs": {
                        "SnapshotId": "snap-111222333444aaabb",
                        "DeleteOnTermination": true,
                        "VolumeType": "gp2",
                        "VolumeSize": 10,
                        "Encrypted": false
                    }
                }
            ],
            "Architecture": "x86_64",
            "ImageLocation": "123456789012/RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-
GP2",
            "RootDeviceType": "ebs",
            "OwnerId": "123456789012",
            "PlatformDetails": "Red Hat Enterprise Linux",
            "UsageOperation": "RunInstances:0010",
            "RootDeviceName": "/dev/sda1",
            "CreationDate": "2019-05-10T13:17:12.000Z",
            "Public": true,
            "ImageType": "machine",
            "Name": "RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-GP2"
        }
    ]
}
```


Verifique los cargos de la AMI en su factura

Para garantizar que no incurra en costos imprevistos, puede verificar que la información de facturación de una instancia en su Informe de uso y costo de AWS (CUR) coincida con la información de facturación asociada a la AMI que utilizó para iniciar la instancia.

Para verificar la información de facturación, busque el ID de la instancia en el CUR y compruebe el valor correspondiente en la columna `lineitem/Operation`. El valor debe coincidir con el valor de la Operación de uso asociada a la AMI.

Por ejemplo, la AMI `ami-0123456789EXAMPLE` tiene la siguiente información de facturación:

- Detalles de la plataforma = `Red Hat Enterprise Linux`
- Operación de uso = `RunInstances:0010`

Si ha iniciado una instancia con esta AMI, puede encontrar el ID de instancia en su CUR y verificar el valor correspondiente en la columna `lineitem/Operation`. En este ejemplo, el valor debería ser `RunInstances:0010`.

Cuotas de IAM

Las siguientes cuotas se aplican a la creación y el uso compartido de AMI. Las cuotas se aplican por Región de AWS.

Nombre de la cuota	Descripción	Cuota predeterminada por región
AMI	El número máximo de AMI públicas y privadas permitido por región. Esto incluye las AMI disponibles, pendientes y deshabilitadas, así como las AMI de la Papelera de reciclaje.	50 000
AMI públicas	El número máximo de AMI públicas, incluidas las de la papelera de reciclaje, permitido por región.	5
Uso compartido de AMI	La cantidad máxima de entidades (organizaciones, unidades organizativas [OU] y cuentas) con las que se puede compartir una AMI en una región. Tenga en cuenta que, si comparte una AMI con una organización o una unidad organizativa, el número	1 000

Nombre de la cuota	Descripción	Cuota predeterminada por región
	de cuentas en cualquiera de estas últimas no se tendrá en cuenta para la cuota.	

Si supera sus cuotas y quiere crear o compartir más AMI, puede hacer lo siguiente:

- Si supera la cuota total de AMI o AMI públicas, considere la posibilidad de anular el registro de las imágenes no utilizadas.
- Si supera la cuota de AMI públicas, considere la posibilidad de convertir una o más AMI en privadas.
- Si supera la cuota de uso compartido de AMI, considere la posibilidad de compartir las AMI con una organización o unidad organizativa en lugar de con cuentas independientes.
- Solicite un aumento de cuota de las AMI.

Solicitud de un aumento de cuota de las AMI

Si necesita incrementar la cuota predeterminada de AMI, puede solicitar un aumento.

Para solicitar un aumento de cuota de las AMI

1. Abra la consola de Service Quotas en https://console.aws.amazon.com/servicequotas/.
2. En el panel de navegación, elija AWS servicios.
3. Elija Amazon Elastic Compute Cloud (Amazon EC2) en la lista o escriba el nombre del servicio en el cuadro de búsqueda.
4. Elija la cuota de AMI para solicitar un aumento. Las cuotas de AMI que puede seleccionar son:
   - AMI
   - AMI públicas
   - Uso compartido de AMI
5. Elija Solicitar aumento de cuota.
6. En Cambiar el valor de la cuota, ingrese el nuevo valor y, a continuación, seleccione Solicitar.

Para ver las solicitudes pendientes o resueltas recientemente, elija Panel en el panel de navegación. Para las solicitudes pendientes, seleccione el estado de la solicitud para abrir la recepción de solicitud. El estado inicial de una solicitud es Pendiente. Cuando el estado cambie a Cuota solicitada, verá el número de caso en Número de caso del Centro de soporte. Elija el número de caso para abrir el ticket para su solicitud.

Una vez resuelta la solicitud, Valor de cuota aplicada para la cuota se establece en el nuevo valor.

Para obtener más información, consulte la Guía del usuario de Service Quotas.

Instancias de Amazon EC2

Antes de iniciar un entorno de producción, es necesario responder a las preguntas siguientes.

P. ¿Qué tipo de instancias responde mejor a mis necesidades?

Amazon EC2 proporciona distintos tipos de instancias que permiten elegir la capacidad de CPU, memoria, almacenamiento y red que necesita para ejecutar las aplicaciones. Para obtener más información, consulte Tipos de instancias de Amazon EC2.

P. ¿Qué opción de compra responde mejor a mis necesidades?

Amazon EC2 es compatible con instancias bajo demanda (predeterminado), instancias de spot e instancias reservadas. Para obtener más información, consulte Opciones de compra de instancias.

P. ¿Qué tipo de volumen raíz responde a mis necesidades?

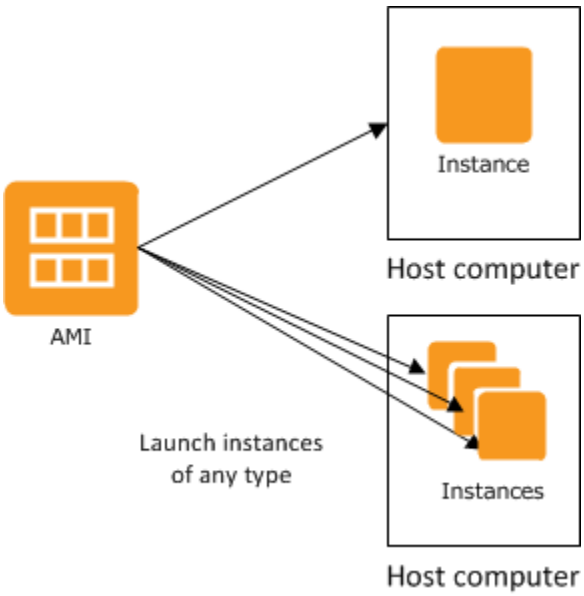
Cada instancia tiene respaldo en el almacén de instancias o en Amazon EBS. Seleccione una AMI según el tipo de volumen raíz que necesite. Para obtener más información, consulte Almacenamiento para el dispositivo raíz.

P. ¿Puedo administrar de forma remota una flota de instancias de EC2 y máquinas en un entorno híbrido?

AWS Systems Manager le permite administrar de forma remota y segura la configuración de sus instancias de Amazon EC2 y las instancias y máquinas virtuales (VM) en las instalaciones en entornos híbridos, incluidas las VM de otros proveedores en la nube. Para obtener más información, consulte la Guía del usuario de AWS Systems Manager.

instancias y AMI

Una Imagen de máquina de Amazon (AMI) es una plantilla que contiene una configuración de software (por ejemplo, un sistema operativo, un servidor de aplicaciones y aplicaciones). Desde una AMI, se inicia una instancia que es una copia de la AMI que se ejecuta como un servidor virtual en la nube. Puede iniciar varias instancias de una AMI, como se muestra en la figura siguiente.



Las instancias siguen en ejecución hasta que se detienen, se terminan, se ponen en hibernación o experimentan algún error. Si una instancia falla, puede iniciar una nueva desde la AMI.

instancias

Una instancia es un servidor virtual en la nube. Su configuración cuando se inicia es una copia de la AMI que especificó al iniciar la instancia.

Puede iniciar distintos tipos de instancias desde una única AMI. Básicamente, un tipo de instancia determina el hardware del ordenador host utilizado para la instancia. Cada tipo de instancia ofrece diferentes capacidades de memoria y computación. Seleccione un tipo de instancias según la cantidad de memoria y de potencia de cómputo que precise para la aplicación o el software que tiene previsto ejecutar en la instancia. Para obtener especificaciones detalladas, consulte Especificaciones en la Guía de tipos de instancias de Amazon EC2. Para obtener más información sobre precios, consulte Precios de Amazon EC2 bajo demanda.

Después de iniciar una instancia, su aspecto es el de un host tradicional y puede interactuar con ella como lo haría con un equipo. Tiene control total de las instancias; puede usar sudo para ejecutar comandos que requieren privilegios raíz.

La cuenta de AWS tiene un límite de instancias que se pueden tener en ejecución. Para obtener más información sobre este límite y el modo de solicitar un aumento, consulte ¿Cuántas instancias puedo ejecutar en Amazon EC2? en las preguntas frecuentes generales de Amazon EC2.

Almacenamiento de instancias

El dispositivo raíz de la instancia contiene la imagen usada para arrancar la instancia. El dispositivo raíz es un volumen Amazon Elastic Block Store (Amazon EBS) o un volumen de almacén de instancias. Para obtener más información, consulte Volumen raíz de la instancia de Amazon EC2.

La instancia puede incluir volúmenes de almacenamiento local, conocidos como volúmenes de almacén de instancias, que puede configurar en el momento de la inicialización con mapeo de dispositivos de bloques. Para obtener más información, consulte Mapeos de dispositivos de bloques. Una vez que estos volúmenes se han agregado a la instancia y mapeado, están disponibles para que los monte y utilice. Si la instancia da error o si se para o termina, los datos de estos volúmenes se pierden; por tanto, el mejor uso que se puede dar a estos volúmenes es para datos temporales. Para proteger los datos importantes, es conveniente utilizar una estrategia de replicación entre varias instancias o bien almacenar los datos persistentes en volúmenes de Amazon S3 o Amazon EBS. Para obtener más información, consulte Opciones de almacenamiento para sus instancias de Amazon EC2.

Prácticas recomendadas de seguridad

- Utilice AWS Identity and Access Management (IAM) para controlar el acceso a los recursos de AWS, incluidas las instancias. Para obtener más información, consulte Identity and Access Management para Amazon EC2.
- Restrinja el acceso permitiendo solo el acceso a los puertos de la instancia a redes u hosts de confianza. Por ejemplo, puede restringir el acceso SSH restringiendo el tráfico entrante en el puerto 22. Para obtener más información, consulte Grupos de seguridad de Amazon EC2 para instancias EC2.
- Revise las reglas de los grupos de seguridad con regularidad y asegúrese de que aplica el principio de privilegio mínimo: abra únicamente los permisos que necesite. También puede crear diferentes grupos de seguridad para trabajar con instancias que tienen distintos requisitos de seguridad. Considere la creación de un grupo de seguridad bastión que permita inicios de sesión externos y mantenga el resto de las instancias en un grupo que no permita los inicios de sesión externos.
- Deshabilite los inicios de sesión basados en contraseña para las instancias iniciadas desde la AMI. Las contraseñas se pueden encontrar o revelar, y constituyen un riesgo para la seguridad. Para obtener más información, consulte Deshabilitación de los inicios de sesión remotos mediante contraseña para el usuario raíz. Para obtener más información acerca del modo de compartir las AMI de manera segura, consulte AMI compartidas.

Detener y finalizar instancias

Puede parar o terminar una instancia en ejecución en cualquier momento.

Detener una instancia

Cuando se para una instancia, se lleva a cabo un cierre normal y después una transición a un estado `stopped`. Todos los volúmenes de Amazon EBS se mantienen adjuntos y puede iniciar la instancia de nuevo más adelante.

No se cobra por el uso adicional de la instancia mientras se encuentre en un estado detenido. Se cobra por cada transición de un estado detenido a un estado en ejecución. Si el tipo de instancia cambió mientras estaba detenida, se cobra la tasa del nuevo tipo de instancia después de que la inicie. También se cobra por el almacenamiento en Amazon EBS asociado para la instancia, incluido el volumen de dispositivo raíz.

Cuando una instancia está en estado detenido, puede adjuntar o separar volúmenes de Amazon EBS. También puede crear una AMI desde la instancia y cambiar el kernel, el disco RAM y el tipo de instancia.

Finalizar una instancia

Cuando se termina una instancia, esta se cierra de forma normal. El volumen de dispositivo raíz se elimina de forma predeterminada, pero cualquier volumen de Amazon EBS asociado se conserva de forma predeterminada, determinada por la configuración de atributo `deleteOnTermination` de cada volumen. La propia instancia se elimina y no podrá iniciarla de nuevo en un momento posterior.

Para evitar que la instancia termine de forma accidental, puede deshabilitar su terminación. Si lo hace, asegúrese de que el atributo `disableApiTermination` está establecido en `true` para la instancia. Para controlar el comportamiento del cierre de una instancia, como `shutdown -h` en Linux o `shutdown` en Windows, establezca el atributo `instanceInitiatedShutdownBehavior` de la instancia en `stop` o `terminate` como se desee. Las instancias con volúmenes Amazon EBS para el dispositivo raíz tienen el valor predeterminado `stop` y las instancias con dispositivos raíz de almacén de instancias siempre terminan como resultado del cierre de una instancia.

Para obtener más información, consulte Ciclo de vida de la instancia.

> **Note**
>
> Algunos recursos de AWS, como los volúmenes de Amazon EBS y las direcciones IP elásticas, generan costos con independencia del estado de la instancia. Para obtener más

información, consulte Evitar cargos inesperados en la Guía del usuario de AWS Billing. Para obtener más información acerca del costo de Amazon EBS, consulte Precio de Amazon EBS.

AMI

Amazon Web Services (AWS) publica imágenes de máquina de Amazon (AMI) con configuraciones de software habituales para uso público. Además, los miembros de la comunidad de desarrolladores de AWS han publicado AMI personalizadas. También se pueden crear AMI personalizadas; con ellas, se pueden iniciar, de manera rápida y sencilla, nuevas instancias con todo lo necesario. Por ejemplo, si la aplicación es un sitio web o un servicio web, la AMI podría incluir un servidor web, el contenido estático asociado y el código para las páginas dinámicas. Como resultado, después de iniciar una instancia desde esta AMI, el servidor web se inicia y la aplicación está lista para aceptar solicitudes.

Todas las AMI se clasifican como respaldadas por Amazon EBS, lo que significa que el dispositivo raíz de la instancia iniciada desde la AMI es un volumen de Amazon EBS o respaldada por el almacén de instancias, lo que significa que el dispositivo raíz de la instancia iniciada desde la AMI es un volumen de almacén de instancias creada a partir de una plantilla almacenada en Amazon S3.

La descripción de una AMI indica el tipo de dispositivo raíz (`ebs` o `instance store`). Esto es importante porque hay diferencias significativas respecto a lo que se puede hacer con cada tipo de AMI. Para obtener más información sobre estas diferencias, consulte Almacenamiento para el dispositivo raíz.

Puede anular el registro de una AMI cuando haya terminado de usarla. Después de anular el registro de una AMI, no puede utilizarla para iniciar nuevas instancias. Las instancias iniciadas desde la AMI no se verán afectadas. Por lo tanto, si también ha terminado con las instancias iniciadas desde estas AMI, debe terminarlas.

Tipos de instancias de Amazon EC2

Cuando se lanza una instancia, el tipo de instancia que especifique determinará el hardware del equipo host utilizado para la instancia. Cada tipo de instancia ofrece distintas características de computación, memoria y almacenamiento, y se agrupa en una familia de instancias en función de dichas características. Seleccione un tipo de instancia en función de los requisitos de la aplicación o del software que tenga previsto ejecutar en la instancia.

Amazon EC2 dedica algunos recursos del ordenador host, como CPU, memoria y almacenamiento de instancias, a una instancia concreta. Amazon EC2 comparte otros recursos del ordenador host,

como la red y el subsistema de disco, entre las instancias. Si cada instancia en un equipo host trata de utilizar la mayor cantidad posible de estos recursos compartidos, cada una recibe una parte igual de dicho recurso. Sin embargo, cuando un recurso está infrautilizado, una sola instancia puede consumir una parte mayor de dicho recurso mientras esté disponible.

Cada tipo de instancia obtiene un rendimiento mínimo superior o inferior de un recurso compartido. Por ejemplo, los tipos de instancias con un alto rendimiento de E/S tienen una mayor asignación de recursos compartidos. Asignar una mayor proporción de recursos compartidos también reduce la variación de rendimiento de E/S. Para la mayoría de las aplicaciones, un rendimiento de E/S moderado es más que suficiente. No obstante, para las aplicaciones que requieran un rendimiento de E/S mayor o más uniforme, piense en utilizar un tipo de instancia con un rendimiento de E/S superior.

Contenido

Tipos de instancias disponibles

Amazon EC2 proporciona una amplia selección de tipos de instancias optimizados para adaptarse a diferentes casos de uso. Los tipos de instancias tienen distintos tipos de combinaciones de CPU, memoria, almacenamiento y capacidad de red. También, brindan la flexibilidad para elegir la combinación adecuada de recursos para las aplicaciones. Cada tipo de instancia incluye uno o varios tamaños de instancia, lo que permite escalar los recursos según los requisitos de la carga de trabajo de destino. Para obtener más información sobre las características y los casos de uso, consulte Detalles de los tipos de instancias de Amazon EC2.

Convenciones de nomenclatura de tipo de instancia

Los nombres se basan en la familia de la instancia, la generación, la familia de procesadores, la capacidades y el tamaño. Para obtener más información, consulte Convenciones de nomenclatura en la Guía de tipos de instancias de Amazon EC2.

Buscar un tipo de instancia

Para determinar los tipos de instancias que cumplen con sus requisitos, como regiones admitidas, recursos de computación o recursos de almacenamiento, consulte Búsqueda de un tipo de instancia de Amazon EC2 y las especificaciones de tipos de instancia de Amazon EC2 en la Guía de tipos de instancia de Amazon EC2.

instancias de generación actual

- De uso general: M5 | M5a | M5ad | M5d | M5dn | M5n | M5zn | M6a | M6g | M6gd | M6i | M6id | M6idn | M6in | M7a | M7g | M7gd | M7i | M7i-flex | Mac1 | Mac2 | Mac2-m2 | Mac2-m2pro | T2 | T3 | T3a | T4g
- Optimizadas para la computación: C5 | C5a | C5ad | C5d | C5n | C6a | C6g | C6gd | C6gn | C6i | C6id | C6in | C7a | C7g | C7gd | C7gn | C7i | C7i-flex
- Optimizadas para la memoria: R5 | R5a | R5ad | R5b | R5d | R5dn | R5n | R6a | R6g | R6gd | R6i | R6idn | R6in | R6id | R7a | R7g | R7gd | R7i | R7iz | U-3tb1 | U-6tb1 | U-9tb1 | U-12tb1 | U-18tb1 | U-24tb1 | U7i-12tb | U7in-16tb | U7in-24tb | U7in-32tb | X1 | X2gd | X2idn | X2iedn | X2iezn | X1e | z1d
- Optimizadas para el almacenamiento: D2 | D3 | D3en | H1 | I3 | I3en | I4g | I4i | Im4gn | Is4gen
- De computación acelerada: DL1 | DL2q | F1 | G4ad | G4dn | G5 | G5g | G6 | Gr6 | Inf1 | Inf2 | P2 | P3 | P3dn | P4d | P4de | P5 | Trn1 | Trn1n | VT1
- De computación de alto rendimiento: Hpc6a | Hpc6id | Hpc7a | Hpc7g

instancias de generaciones anteriores

- De uso general: A1 | M1 | M2 | M3 | M4 | T1
- Optimizadas para la computación: C1 | C3 | C4
- Optimizadas para la memoria: R3 | R4
- Optimizadas para el almacenamiento: I2
- De computación acelerada: G3

Especificaciones de hardware

Para obtener especificaciones detalladas de los tipos de instancias, consulte Especificaciones en la Guía de tipos de instancias de Amazon EC2. Para obtener más información sobre precios, consulte Precios de Amazon EC2 bajo demanda.

Para determinar qué tipo de instancia es el más adecuado para sus necesidades, le recomendamos que lance una instancia y utilice su propia aplicación de referencia. Como paga por segundo de instancia, resulta conveniente y económico probar varios tipos de instancias antes de tomar una decisión. Si sus necesidades cambian, incluso después de tomar una decisión, puede ajustar el tipo de instancia posteriormente. Para obtener más información, consulte Cambie el tipo de instancia.

Características del procesador Intel

Las instancias Amazon EC2 que se ejecutan en procesadores Intel pueden incluir las siguientes características. No todas las siguientes características del procesador son compatibles con todos los tipos de instancias. Para obtener información detallada acerca de las características disponibles para cada tipo de instancia, consulte Tipos de instancias de Amazon EC2.

- Intel AES New Instructions (AES-NI) — El conjunto de instrucciones de cifrado Intel AES-NI mejora el algoritmo estándar de cifrado avanzado (AES) original para ofrecer una protección de los datos más rápida y mayor seguridad. Todas las instancias de EC2 de la generación actual soportan esta característica del procesador.
- Extensiones vectoriales avanzadas de Intel (Intel AVX, Intel AVX2 y AVX-512) — Intel AVX e Intel AVX2 son extensiones de conjuntos de instrucciones de 256 bits, mientras que Intel AVX-512 es una extensión de conjuntos de instrucciones de 512 bits. Están diseñadas para aplicaciones con un uso intensivo de coma flotante (FP). Las instrucciones Intel AVX mejoran el rendimiento de aplicaciones de procesado de audio/video e imágenes, simulaciones científicas, análisis financieros y análisis y modelado en 3D. Estas características solo están disponibles en las instancias iniciadas con las AMI HVM.
- Tecnología Intel Turbo Boost — Los procesadores de la tecnología Intel Turbo Boost ejecutan núcleos automáticamente más rápido que la frecuencia de operación básica.
- Intel Deep Learning Boost (Intel DL Boost) — Acelera los casos de uso del aprendizaje profundo de IA. Los procesadores Intel Xeon Scalable de segunda generación amplían las instrucciones Intel AVX-512 con una nueva instrucción de red neuronal vectorial (VNNI/INT8) que aumenta significativamente el rendimiento de la inferencia del aprendizaje profundo en comparación con los procesadores Intel Xeon Scalable de la generación anterior (con FP32), para el reconocimiento o

la segmentación de imágenes, la detección de objetos, el reconocimiento de voz, la traducción de idiomas, los sistemas de recomendaciones, el aprendizaje mediante refuerzo y más. Puede que VNNI no sea compatible con todas las distribuciones de Linux.

Las siguientes instancias admiten VNNI: `M5n`, `R5n`, `M5dn`, `M5zn`, `R5b`, `R5dn`, `D3`, `D3en` y `C6i`. Las instancias `C5` y `C5d` admiten VNNI solo para las instancias `12xlarge`, `24xlarge` y `metal`.

Las convenciones de nomenclatura de las CPU de 64 bits del sector pueden inducir a errores. El fabricante de chips, Advanced Micro Devices (AMD), desarrolló la primera arquitectura de 64 bits comercialmente viable basada en conjunto de instrucciones de Intel x86. Por ello, esta arquitectura suele recibir el nombre de AMD64 con independencia de quién sea el fabricante del chip. Varios distribuidores de Windows y Linux llevan a cabo esta práctica. Esto explica por qué la información interna del sistema de una instancia de Ubuntu o de Windows muestra la arquitectura de la CPU como AMD64, a pesar de que las instancias se ejecutan en equipos de Intel.

Procesadores AWS Graviton

AWS Graviton es una familia de procesadores diseñada para ofrecer la mejor relación precio-rendimiento para sus cargas de trabajo que se ejecutan en instancias de Amazon EC2.

Para obtener más información, consulte Introducción a Graviton.

AWS Trainium

Las instancias alimentadas por AWS Trainium están diseñadas específicamente para el entrenamiento en aprendizaje profundo rentable y de alto rendimiento. Puede utilizar estas instancias para entrenar el procesamiento del lenguaje natural, la visión artificial y los modelos de recomendación que se utilizan en un amplio conjunto de aplicaciones, como el reconocimiento de voz, la recomendación, la detección de fraudes y la clasificación de imágenes y videos. Use los flujos de trabajo existentes en marcos de ML populares, como PyTorch y TensorFlow.

Inferentia AWS

Las instancias alimentas por AWS Inferentia están diseñadas para acelerar el machine learning. Proporcionan inferencias de machine learning de alto rendimiento y baja latencia. Estas instancias están optimizadas para implementar modelos de aprendizaje profundo (DL) para aplicaciones, como procesamiento de lenguaje natural, detección y clasificación de objetos, personalización y filtrado de contenido y reconocimiento de voz.

Hay una variedad de formas con las que puede comenzar.

- Utilice SageMaker, un servicio totalmente administrado que es la forma más fácil de comenzar con los modelos de machine learning. Para obtener más información, consulte Introducción a SageMaker en la Guía para desarrolladores de Amazon SageMaker.
- Inicie una instancia Inf1 o Inf2 mediante la AMI de deep learning. Para obtener más información, consulte AWS Inferentia con DLAMI en la Guía para desarrolladores de AWS Deep Learning AMI.
- Lance una instancia Inf1 o Inf2 con su propia AMI e instale el Neuron SDK de AWS, que permite compilar, ejecutar y perfilar modelos de deep learning para la Inferentia de AWS.
- Lance una instancia de contenedor mediante una instancia Inf1 o Inf2 y una AMI de Amazon ECS optimizada. Para obtener más información, consulte AMI de Amazon Linux 2 (Inferentia) en la Amazon Elastic Container Service Developer Guide.
- Cree un clúster de Amazon EKS con nodos que ejecuten instancias Inf1. Para obtener más información, consulte Soporte de Inferentia en la Guía del usuario de Amazon EKS.

Tipos de virtualización de AMI

El tipo de virtualización de la instancia está determinado por la AMI que utilice para iniciarla. Los tipos de instancias de la generación actual solo admiten máquinas virtuales de hardware (HVM). Algunos tipos de instancias de generaciones anteriores admiten paravirtual (PV) y algunas regiones de AWS son compatibles con instancias PV. Para obtener más información, consulte Tipos de virtualización de AMI.

Para obtener el máximo rendimiento, le recomendamos que utilice una AMI HVM. Además, las AMI HVM son necesarias para beneficiarse de las redes mejoradas. La virtualización HVM utiliza la tecnología asistida por hardware proporcionada por la plataforma de AWS. Con la virtualización HVM, la VM invitada se ejecuta como si se encontrase en una plataforma de hardware nativa, salvo que continúa utilizando la red PV y los controladores de almacenamiento para mejorar el rendimiento.

Búsqueda de un tipo de instancia de Amazon EC2

Para poder iniciar una instancia, debe seleccionar el tipo de instancia que quiere usar. El tipo de instancia que elija puede depender de los recursos que necesite la carga de trabajo; por ejemplo, recursos de computación, memoria o almacenamiento. Puede que sea útil identificar varios tipos de instancias que podrían adaptarse a la carga de trabajo y evaluar su rendimiento en un entorno de prueba. No hay ningún sustituto para medir el rendimiento de una aplicación bajo carga.

Si ya tiene instancias de EC2 en ejecución, puede utilizar AWS Compute Optimizer para obtener recomendaciones sobre los tipos de instancias que debería utilizar para mejorar el rendimiento, ahorrar dinero o ambas cosas. Para obtener más información, consulte the section called “Para cargas de trabajo existentes”.

Tareas

- Buscar un tipo de instancia mediante la consola
- Buscar un tipo de instancia con la AWS CLI

Buscar un tipo de instancia mediante la consola

Puede buscar un tipo de instancia que satisfaga sus necesidades utilizando la consola de Amazon EC2.

Para buscar un tipo de instancia mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la barra de navegación, seleccione la región en la que se iniciarán las instancias. Puede seleccionar cualquier región disponible, independientemente de su ubicación.
3. En el panel de navegación, elija Instances Types (Tipos de instancia).
4. (Opcional) Elija el icono de preferencias (engranaje) para seleccionar los atributos del tipo de instancia que desea visualizar, como el Precios de Linux bajo demanda y, a continuación, elija Confirmar. Como alternativa, puede seleccionar el nombre de un tipo de instancia para abrir su página de detalles y ver todos los atributos disponibles a través de la consola. La consola no muestra todos los atributos disponibles a través de la API o la línea de comandos.
5. Utilice los atributos de tipo de instancia para filtrar la lista de tipos de instancia mostrados solo a los tipos de instancia que satisfagan sus necesidades. Por ejemplo, puede filtrar por los siguientes atributos:

    - Availability zones (Zonas de disponibilidad): nombre de la zona de disponibilidad, la zona local o la zona Wavelength. Para obtener más información, consulte the section called “Regiones y zonas”.
    - vCPUs o Cores (Núcleos): número de vCPU o núcleos.
    - Memory (GiB) (Memoria [GiB]): tamaño de la memoria en GiB.
    - Network performance (Rendimiento de la red): rendimiento de la red en gigabits.

- Local instance storage (Almacenamiento de instancias local): indica si el tipo de instancia tiene almacenamiento de instancias local (`true` | `false`).

6. (Opcional) Para ver una comparación en paralelo, seleccione la casilla de verificación de varios tipos de instancias. La comparación se muestra en la parte inferior de la pantalla.
7. (Opcional) Para guardar la lista de tipos de instancias en un archivo de valores separados por comas (.csv) con objeto de realizar una revisión posterior, elija Actions (Acciones), Download list CSV (Descargar CSV de lista). El archivo incluye todos los tipos de instancia que coinciden con los filtros definidos.
8. (Opcional) Para iniciar instancias utilizando un tipo de instancia que se ajuste a sus necesidades, seleccione la casilla de verificación del tipo de instancia y elija Actions (Acciones), Launch instance (iniciar instancia). Para obtener más información, consulte Lance una instancia con el nuevo asistente de inicialización de instancias.

Buscar un tipo de instancia con la AWS CLI

Puede usar comandos de la AWS CLI para Amazon EC2 para buscar un tipo de instancia que satisfaga sus necesidades.

Para buscar un tipo de instancia con la AWS CLI

1. Si aún no lo ha hecho, instale AWS CLI. Para obtener más información, consulte la Guía del usuario de AWS Command Line Interface.
2. Utilice el comando describe-instance-types para filtrar los tipos de instancia en función de los atributos de instancia. Por ejemplo, puede utilizar el siguiente comando para que se muestren únicamente los tipos de instancias de la generación actual con 64 GiB (65 536 MiB) de memoria.

```
aws ec2 describe-instance-types --filters "Name=current-generation,Values=true"
 "Name=memory-info.size-in-mib,Values=65536" --query "InstanceTypes[*].
[InstanceType]" --output text | sort
```

3. Utilice el comando describe-instance-type-offerings para filtrar los tipos de instancias ofrecidos por ubicación (región o zona). Por ejemplo, puede utilizar el siguiente comando para que se muestren los tipos de instancias ofrecidos en la zona especificada.

```
aws ec2 describe-instance-type-offerings --location-type "availability-
zone" --filters Name=location,Values=us-east-2a --region us-east-2 --query
 "InstanceTypeOfferings[*].[InstanceType]" --output text | sort
```

4. Una vez que haya localizado los tipos de instancias que se ajustan a sus necesidades, guarde la lista, para poder utilizar esos tipos de instancias cuando lance instancias. Para obtener más información, consulte Cómo iniciar su instancia en la Guía del usuario de AWS Command Line Interface.

Obtener recomendaciones para un tipo de instancia

Las siguientes herramientas pueden ayudarlo a seleccionar los tipos de instancias óptimos para sus cargas de trabajo nuevas o existentes:

- Cargas de trabajo nuevas: el buscador de tipos de instancias EC2 tiene en cuenta su caso de uso, el tipo de carga de trabajo, las preferencias del fabricante de la CPU y la forma en que prioriza el precio y el rendimiento, así como los parámetros adicionales que puede especificar. A continuación, utiliza estos datos para proporcionar orientación y sugerencias sobre los tipos de instancias de Amazon EC2 que mejor se adapten a sus nuevas cargas de trabajo.
- Cargas de trabajo existentes: AWS Compute Optimizer analiza las especificaciones de instancia existentes y las métricas de utilización. A continuación, utiliza los datos compilados para recomendar qué tipos de instancia de Amazon EC2 se optimizan en cuanto a costos o rendimiento, o ambos, para sus cargas de trabajo existentes.

Obtenga recomendaciones de tipos de instancias:

- Obtención de recomendaciones de tipos de instancias para una nueva carga de trabajo
- Obtención de recomendaciones de tipos de instancias para una carga de trabajo existente

Obtención de recomendaciones de tipos de instancias para una nueva carga de trabajo

El buscador de tipos de instancias EC2 tiene en cuenta su caso de uso, el tipo de carga de trabajo, las preferencias del fabricante de la CPU y la forma en que prioriza el precio y el rendimiento, así como los parámetros adicionales que puede especificar. A continuación, utiliza estos datos para proporcionar orientación y sugerencias sobre los tipos de instancias de Amazon EC2 que mejor se adapten a sus nuevas cargas de trabajo.

Con tantos tipos de instancias disponibles, encontrar los tipos de instancias adecuados para su carga de trabajo puede ser complejo y llevar mucho tiempo. Al utilizar el buscador de tipos de instancias

EC2, puede mantenerse actualizado con los tipos de instancias más recientes y conseguir la mejor relación entre precio y rendimiento para sus cargas de trabajo.

En este tema se describe cómo obtener orientación y sugerencias para tipos de instancias EC2 a través de la consola de Amazon EC2. También puede dirigirse directamente a Amazon Q para solicitar asesoramiento sobre los tipos de instancias. Para obtener más información, consulte la Guía del usuario de Amazon Q Developer.

Si busca recomendaciones de tipos de instancias para una carga de trabajo existente, utilice AWS Compute Optimizer. Para obtener más información, consulte Obtención de recomendaciones de tipos de instancias para una carga de trabajo existente.

Uso del buscador de tipos de instancias EC2

En la consola de Amazon EC2, puede obtener sugerencias de tipos de instancias en el buscador de tipos de instancias EC2 del asistente de inicialización de instancias, al crear una plantilla de inicialización o en la página Tipos de instancias.

Utilice las siguientes instrucciones para obtener orientación y sugerencias sobre los tipos de instancias EC2 mediante el buscador de tipos de instancias EC2 en la consola de Amazon EC2. Para ver una animación de los pasos, consulte Ver una animación: Cómo obtener sugerencias de tipos de instancias mediante el buscador de tipos de instancias EC2.

Para obtener sugerencias de tipos de instancias mediante el buscador de tipos de instancias EC2

1. Inicie el proceso mediante una de las siguientes opciones:
   - Siga el procedimiento para Iniciar una instancia. Junto a Tipo de instancia, seleccione el enlace Obtener asesoramiento.
   - Siga el procedimiento para crear una plantilla de inicialización. Junto a Tipo de instancia, seleccione el enlace Obtener asesoramiento.
   - En el panel de navegación, seleccione Tipos de instancias y, a continuación, pulse el botón del Buscador de tipos de instancias.
2. En la pantalla Obtenga consejos sobre la selección del tipo de instancia, haga lo siguiente:
   a. Seleccione las opciones correspondientes para Tipo de carga de trabajo, Caso de uso, Prioridad y Fabricantes de CPU para especificar los requisitos del tipo de instancia.
   b. (Opcional) A fin de especificar requisitos más detallados para la carga de trabajo, haga lo siguiente:

i. Expanda Parámetros avanzados.

ii. Para agregar un parámetro, selecciónelo, elija Agregar y especifique un valor para el parámetro. Repita este paso para cada parámetro adicional que desee agregar. Para no indicar un valor mínimo o máximo, deje el campo vacío.

iii. Para eliminar un parámetro después de agregarlo, seleccione la X ubicada junto al parámetro.

c. Elija Obtener asesoramiento sobre tipos de instancias.

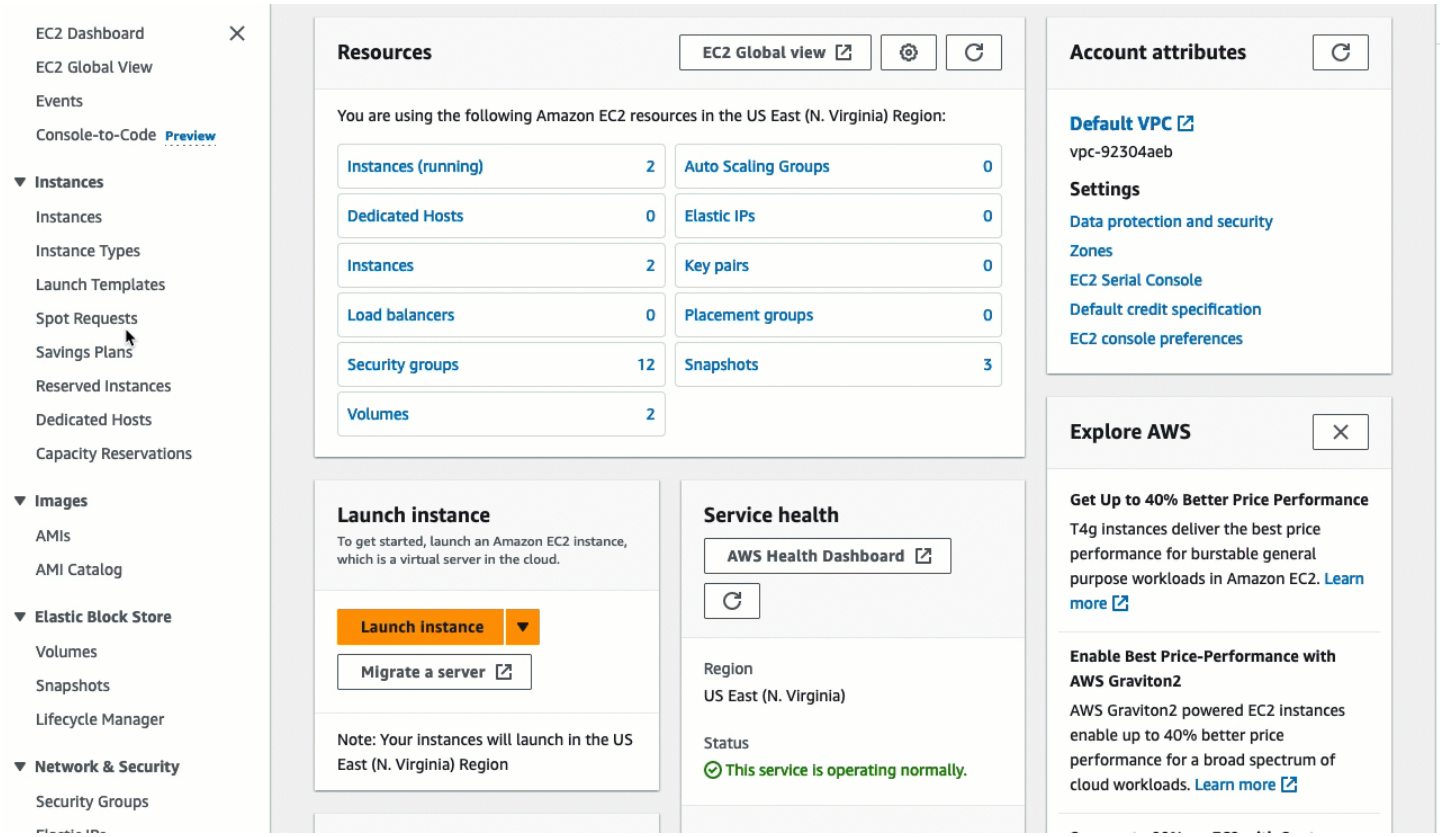
Amazon EC2 le ofrece sugerencias para familias de instancias que se ajusten a los requisitos especificados.

3. Para ver los detalles de cada tipo de instancia dentro de las familias de instancias sugeridas, seleccione Ver detalles de la familia de instancias recomendada.

4. Elija un tipo de instancia que cumpla sus requisitos y, a continuación, seleccione Acciones, Iniciar instancia o Acciones, Crear plantilla de inicialización.

Como alternativa, si ha iniciado el proceso en el asistente de inicialización de instancias o en la página de plantillas de inicialización y prefiere volver al flujo original, tome nota del tipo de instancia que desea usar. A continuación, en el asistente de inicialización de instancias o en la plantilla de inicialización, en Tipo de instancia, elija el tipo de instancia y complete el procedimiento para iniciar una instancia o crear una plantilla de inicialización de instancias.

Ver una animación: Cómo obtener sugerencias de tipos de instancias mediante el buscador de tipos de instancias EC2



Obtención de recomendaciones de tipos de instancias para una carga de trabajo existente

AWS Compute Optimizer ofrece recomendaciones de instancias de Amazon EC2 para ayudarle a mejorar el rendimiento, ahorrar dinero o ambas cosas. Puede utilizar estas recomendaciones para decidir si desea pasar a un nuevo tipo de instancia.

Para hacer recomendaciones, Compute Optimizer analiza las especificaciones de instancia existentes y las métricas de utilización. Los datos recopilados se utilizan a continuación para recomendar qué tipos de instancias de Amazon EC2 son los mejores para gestionar la carga de trabajo existente. Las recomendaciones se devuelven junto con el precio de la instancia por hora.

En este tema se describe cómo ver las recomendaciones a través de la consola de Amazon EC2. Para obtener más información, consulte la Guía del usuario de AWS Compute Optimizer.

> **Note**
>
> Para obtener recomendaciones de Compute Optimizer, primero debe darse de alta en Compute Optimizer. Para obtener más información, consulte el Tutorial de introducción a AWS Compute Optimizer en la Guía del usuario de AWS Compute Optimizer.

Si busca recomendaciones de tipos de instancias para una nueva carga de trabajo, utilice el selector de tipos de instancias de EC2 de Amazon Q. Para obtener más información, consulte Obtención de recomendaciones de tipos de instancias para una nueva carga de trabajo.

Contenido

Limitaciones

Actualmente, Compute Optimizer genera recomendaciones para los tipos de instancias C, D, H, I, M, R, T, X y z. Compute Optimizer no tiene en cuenta otros tipos de instancias. Si utiliza otros tipos de instancias, no se mostrarán en la vista de recomendaciones de Compute Optimizer. Para obtener más información sobre los tipos de instancia admitidos y no admitidos, consulte Requisitos de las instancias de Amazon EC2 en la Guía del usuario de AWS Compute Optimizer.

Resultados

Compute Optimizer clasifica sus conclusiones sobre las instancias de EC2 de la siguiente manera:

- Infraaprovisionada: una instancia de EC2 se considera infraaprovisionada cuando al menos una especificación de la instancia, como la CPU, la memoria o la red, no cumple los requisitos de rendimiento de su carga de trabajo. Las instancias de EC2 infraaprovisionadas podrían producir un rendimiento deficiente de las aplicaciones.
- Aprovisionada en exceso: una instancia de EC2 se considera que está aprovisionada en exceso cuando al menos una especificación de la instancia, como la CPU, la memoria o la red, se puede reducir satisfaciendo al mismo tiempo los requisitos de rendimiento de su carga de trabajo, y

cuando ninguna especificación está infraaprovisionada. Las instancias de EC2 aprovisionadas en exceso podrían ocasionar costos de infraestructura innecesarios.

- Optimizada: una instancia de EC2 se considera optimizada cuando todas las especificaciones de la instancia, como la CPU, la memoria y la red, cumplen los requisitos de rendimiento de la carga de trabajo y la instancia no está aprovisionada en exceso. Una instancia de EC2 optimizada ejecuta sus cargas de trabajo con un rendimiento y un costo de infraestructura óptimos. En el caso de las instancias optimizadas, Compute Optimizer puede recomendar a veces un tipo de instancia de nueva generación.
- Ninguna – no hay recomendaciones para esta instancia. Esto puede ocurrir si hace menos de 12 horas que se dio de alta en Compute Optimizer, cuando la instancia lleva ejecutándose menos de 30 horas o cuando el tipo de instancia no es compatible con Compute Optimizer. Para obtener más información, consulte Limitaciones en la sección anterior.

Ver recomendaciones

Una vez que se haya dado de alta en Compute Optimizer, puede ver los resultados que Compute Optimizer genera para las instancias de EC2 en la consola de EC2. A continuación, puede acceder a la consola de Compute Optimizer para ver las recomendaciones. Si se ha dado de alta recientemente, es posible que los resultados no se reflejen en la consola de EC2 hasta al cabo de 12 horas.

Cómo ver una recomendación para una instancia de EC2 mediante la consola de EC2

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione instancias y, a continuación, el ID de la instancia .
3. En la página de resumen de la instancia, en el banner de AWS Compute Optimizer en la parte inferior de la página, elija Ver detalles.

   La instancia se abre en Compute Optimizer, donde se etiqueta como la instancia Current (Actual). Se proporcionan hasta tres recomendaciones de tipos de instancias diferentes: Option 1 (Opción 1), Option 2 (Opción 2) y Option 3 (Opción 3). La mitad inferior de la ventana muestra datos de métricas recientes de CloudWatch recientes para la instancia actual: CPU utilization (Utilización de CPU), Memory utilization (Utilización de memoria), Network in (Entrada de red) y Network out (Salida de red).
4. (Opcional) En la consola de Compute Optimizer, elija la configuración ()

para cambiar las columnas visibles de la tabla o para ver la información pública de precios de una opción de compra diferente de los tipos de instancias actuales y recomendados.

> **Note**
>
> Si ha comprado una instancia reservada, es posible que su instancia a petición se le facture como una instancia reservada. Antes de cambiar el tipo de instancia actual, evalúe primero el impacto en la utilización y la cobertura de la instancia reservada.

Determine si desea utilizar alguna de las recomendaciones. Decida si desea optimizar las instancias para mejorar el rendimiento, para reducir los costos o para ambas cosas. Para obtener más información, consulte Ver recomendaciones de recursos en la Guía del usuario de AWS Compute Optimizer.

Para ver recomendaciones para todas las instancias de EC2 en todas las regiones a través de la consola de Compute Optimizer

1. Abra la consola de Compute Optimizer en https://console.aws.amazon.com/compute-optimizer/.
2. Elija Ver recomendaciones para todas las instancias de EC2.
3. Puede realizar las siguientes acciones en la página de recomendaciones:

   a. Para filtrar las recomendaciones a una o varias regiones de AWS, escriba el nombre de la región en el cuadro de texto Filter by one or more Regions (Filtrar por una o varias regiones) o elija una o varias regiones en la lista desplegable que aparece.

   b. Para ver las recomendaciones de recursos de otra cuenta, elija Account (Cuenta), y, a continuación, seleccione un ID de cuenta diferente.

      Esta opción solo está disponible si ha iniciado sesión en una cuenta de administración de una organización y se ha dado de alta en todas las cuentas miembro de la organización.

   c. Para borrar los filtros seleccionados, elija Clear filters (Borrar filtros).

   d. Para cambiar la opción de compra que se muestra para los tipos de instancias actuales y recomendados, elija la configuración () y, a continuación, elija instancias bajo demanda, instancias reservadas, 1 año estándar sin anticipos o instancias reservadas, 3 años estándar sin anticipos.

e. Para ver detalles, como recomendaciones adicionales y una comparación de las métricas de utilización, elija el resultado (Under-provisioned (Infraaprovisionada), Over-provisioned (Aprovisionada en exceso) u Optimized (Optimizada)) que aparece junto a la instancia que desee. Para obtener más información, consulte Ver detalles de recursos en la Guía del usuario deAWS Compute Optimizer.

Consideraciones para evaluar recomendaciones

Antes de cambiar un tipo de instancia, tenga en cuenta lo siguiente:

- Las recomendaciones no prevén el uso que hará de ellas. Las recomendaciones se basan en su uso histórico durante el periodo de 14 días más reciente. Asegúrese de elegir un tipo de instancia que crea que va a satisfacer sus necesidades futuras de recursos.
- Céntrese en las métricas gráficas para determinar si el uso real es inferior a la capacidad de la instancia. También puede ver los datos de métricas (promedio, pico, percentil) en CloudWatch para evaluar más detalladamente las recomendaciones de instancias de EC2. Por ejemplo, observe cómo cambian las métricas de porcentaje de CPU durante el día y si hay picos que deben acomodarse. Para obtener más información, consulte Visualización de las métricas disponibles en la Guía del usuario de Amazon CloudWatch.
- Compute Optimizer podría proporcionar recomendaciones para instancias de rendimiento ampliable, que son las instancias T3, T3a y T2. Si amplía su capacidad periódicamente por encima del nivel de referencia, asegúrese de que puede seguir haciéndolo ahora con las vCPU del nuevo tipo de instancia. Para obtener más información, consulte Conceptos clave y definiciones para las instancias de rendimiento ampliables.
- Si ha comprado una instancia reservada, es posible que su instancia a petición se le facture como una instancia reservada. Antes de cambiar el tipo de instancia actual, evalúe primero el impacto en la utilización y la cobertura de la instancia reservada.
- Considere la posibilidad de cambiar a instancias de nueva generación, siempre que sea posible.
- Al migrar a una familia de instancias diferente, asegúrese de que el tipo de instancia actual y el nuevo tipo de instancia sean compatibles, por ejemplo, en cuanto a virtualización, arquitectura o tipo de red. Para obtener más información, consulte Compatibilidad para cambiar el tipo de instancia.
- Por último, considere la calificación de riesgo de rendimiento que se proporciona para cada recomendación. El riesgo de rendimiento indica la cantidad de esfuerzo que puede necesitar invertir para validar si el tipo de instancia recomendado cumple los requisitos de rendimiento de la

carga de trabajo. También es recomendable que realice pruebas de carga y rendimiento rigurosas antes y después de realizar cualquier cambio.

Hay otras consideraciones que deben tenerse en cuenta al cambiar el tamaño de una instancia de EC2. Para obtener más información, consulte Cambie el tipo de instancia.

Recursos adicionales

Para obtener más información:

- Tipos de instancias de Amazon EC2
- Guía del usuario de AWS Compute Optimizer

Cambie el 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). En tal caso, puede cambiar el tamaño de la instancia cambiando el tipo de instancia. Por ejemplo, si su instancia `t2.micro` es demasiado pequeña para su carga de trabajo, puede aumentar su tamaño cambiándola a un tipo de instancia T2 más grande, como `t2.large`. O puede cambiarlo a otro tipo de instancia, como `m5.large`. También puede ser conveniente migrar de un tipo de instancia de una generación anterior a un tipo de instancia de generación actual para sacar partido de algunas características, como la compatibilidad con IPv6.

Si desea una recomendación para un tipo de instancia que sea más apta para manejar su carga de trabajo existente, puede utilizar AWS Compute Optimizer. Para obtener más información, consulte Obtención de recomendaciones de tipos de instancias para una carga de trabajo existente.

Cuando se cambia el tipo de instancia, comenzará a pagar la tarifa del nuevo tipo de instancia. Para conocer las tarifas bajo demanda de todos los tipos de instancias, consulte Precios de Amazon EC2 bajo demanda.

Para agregar almacenamiento adicional a la instancia sin cambiar el tipo de instancia, agregue un volumen de EBS a la instancia. Para obtener más información, consulte Adjunte un volumen de Amazon EBS a una instancia en la Guía del usuario de Amazon EBS.

¿Qué instrucciones seguir?

Existen diferentes instrucciones para cambiar el tipo de instancia. Las instrucciones de uso dependen del volumen raíz de la instancia y de si el tipo de instancia es compatible con la configuración actual de la instancia. Para obtener información acerca de cómo se determina la compatibilidad, consulte Compatibilidad para cambiar el tipo de instancia.

Utilice la siguiente tabla para determinar qué instrucciones seguir.

Volumen raíz	Compatibilidad	Utilice estas instrucciones.
EBS	Compatible	Cambiar el tipo de instancias de una instancia con respaldo de EBS
EBS	No compatible	Cambiar el tipo de instancia mediante la inicialización de una nueva instancia
Almacén de instancias	No aplicable	Cambiar el tipo de instancia de una instancia con respaldo en el almacén de instancias

Consideraciones para los tipos de instancia compatibles

Tenga en cuenta lo siguiente al cambiar el tipo de instancia de una instancia existente:

- Debe detener la instancia con respaldo de Amazon EBS para poder cambiar el tipo de instancia. Asegúrese de tener previsto un tiempo de inactividad mientras la instancia está detenida. El detenimiento y el cambio de tipo de 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 Detención e iniciación de una instancia de Amazon EC2.
- Cuando se para y se inicia una instancia, la trasladamos a un nuevo equipo. Si la instancia tiene una dirección IPv4 pública, liberamos la dirección y le asignamos una nueva dirección IPv4 pública. Si necesita una dirección IPv4 pública que no cambia, utilice una dirección IP elástica.
- No puede cambiar el tipo de instancia de una instancia de spot.
- [Instancias de Windows] Le recomendamos que actualice el paquete de controladores PV de AWS antes de cambiar el tipo de instancia. Para obtener más información, consulte the section called “Actualizar controladores PV”.

- Si la instancia pertenece a un grupo de escalado automático, el servicio Amazon EC2 Auto Scaling marca la instancia detenida como en mal estado y podría terminarla y iniciar una instancia de sustitución. Para evitar esto, puede suspender los procesos de escalado del grupo mientras cambia el tipo de instancia. Para obtener más información, consulte Suspender y reanudar un proceso para un grupo de escalado automático en la Guía del usuario de Amazon EC2 Auto Scaling.
- Cuando cambia el tipo de instancia de una instancia con volúmenes de almacén de instancias de NVMe, es posible que la instancia actualizada tenga volúmenes de almacén de instancias adicionales, ya que todos los volúmenes de almacén de instancias de NVMe están disponibles incluso si no se especifican en la AMI o en la asignación de dispositivos de bloques de instancias. De lo contrario, la instancia actualizada tiene la misma cantidad de volúmenes de almacén de instancias que especificó cuando lanzó la instancia original.
- La cantidad máxima de volúmenes de Amazon EBS que puede adjuntar a una instancia depende del tipo y tamaño de la instancia. No puede cambiar a un tipo o tamaño de instancia que no admita la cantidad de volúmenes que ya están adjuntos a su instancia. Para obtener más información, consulte Límites de volumen de instancias.

Cambiar el tipo de instancias de una instancia con respaldo de EBS

Utilice las instrucciones siguientes para cambiar el tipo de instancia de una instancia con respaldo de EBS si el tipo de instancia que necesita es compatible con la configuración actual de la instancia.

Para cambiar el tipo de instancias de una instancia con respaldo de 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 para cambiar el tipo de instancia.
2. [Instancias de Windows] Si ha configurado la instancia de Windows para que utilice direcciones IP estáticas y cambia la instancia de un tipo que no admite la conexión en red mejorada a un tipo que sí la admite, podría recibir una advertencia sobre un potencial conflicto de dirección IP cuando reconfigure las direcciones IP estáticas. Para evitar esto, habilite DHCP en la interfaz de red de la instancia antes de cambiar el tipo de instancia. Desde la instancia, abra Network and Sharing Center (Centro de redes y recursos compartidos) y Internet Protocol Version 4 (TCP/IPv4) Properties (Propiedades del protocolo de Internet versión 4 [TCP/IPv4]) de la interfaz de red, y elija Obtain an IP address automatically (Obtener una dirección IP automáticamente). Cambie el tipo de instancia y reconfigure las direcciones IP estáticas en la interfaz de red.

3. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
4. En el panel de navegación, seleccione Instancias.
5. Seleccione la instancia y elija Instance State (Estado de la instancia) y Stop instance (Detener instancia). Cuando se le pida que confirme, seleccione Detener. Puede que transcurran unos minutos hasta que la instancia se detenga.
6. Con la instancia aún seleccionada, elija Actions (Acciones), Instance settings (Configuración de la instancia), Change instance type (Cambiar tipo de instancia). Esta opción aparece atenuada si el estado de la instancia no es `stopped`.
7. En la página Change instance type (Cambiar tipo de instancia), realice una de las acciones siguientes:

   a. Para Instance type (Tipo de instancia), seleccione el tipo de instancia que desea.

      Si el tipo de instancia no está en la lista, no es compatible con la configuración de la instancia. En su lugar, utilice las siguientes instrucciones: Cambiar el tipo de instancia mediante la inicialización de una nueva instancia.

   b. (Opcional) Si el tipo de instancia que ha elegido admite la optimización de EBS, seleccione EBS-optimized (Optimizada para EBS) para habilitar la optimización de EBS o anule la selección EBS-optimized (Optimizada para EBS) para deshabilitarla. Si el tipo de instancia que ha seleccionado está optimizada para EBS de forma 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 iniciar la instancia, selecciónela y elija Instance state (Estado de la instancia) y Start instance (Iniciar instancia). Puede que transcurran unos minutos hasta que la instancia pase al estado `running`. Si la instancia no se inicia, consulte Solución de problemas de cambio del tipo de instancia.
9. [Instancias de Windows] Si la instancia ejecuta Windows Server 2016 o Windows Server 2019 con EC2Launch v1, conéctese a su instancia de Windows y ejecute el siguiente script de EC2Launch PowerShell para configurar la instancia después de cambiar el tipo de instancia.

> **Important**
>
> La contraseña del administrador se restablecerá cuando habilite el script de inicialización EC2 de la instancia. Puede modificar el archivo de configuración para deshabilitar el restablecimiento de la contraseña del administrador especificándolo en la configuración de las tareas de inicialización. Para obtener información sobre cómo deshabilitar

el restablecimiento de contraseñas, consulte Configurar las tareas de inicialización (EC2launch) o Cambiar la configuración (EC2Launch v2).

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
Schedule
```

Cambiar el tipo de instancia mediante la inicialización de una nueva instancia

Si la configuración actual de la instancia respaldada por EBS es incompatible con el tipo de instancia nuevo que desea, no podrá cambiar el tipo de instancia de la instancia original. En su lugar, debe iniciar una nueva instancia con una configuración que sea compatible con el nuevo tipo de instancia que desea y, luego, migrar su aplicación a la nueva instancia. Por ejemplo, si ha iniciado la instancia original desde una AMI PV, pero desea cambiar a un tipo de instancia de generación actual que requiere una AMI de HVM, tendrá que iniciar una nueva instancia desde una AMI de HVM. Para obtener información acerca de cómo se determina la compatibilidad, consulte Compatibilidad para cambiar el tipo de instancia.

Para migrar la aplicación a una nueva instancia, haga lo siguiente:

- Haga una copia de seguridad de los datos de su instancia original.
- Lance una nueva instancia con una configuración que sea compatible con el nuevo tipo de instancia que desea y adjunte los volúmenes de EBS que se hayan adjuntado a la instancia original.
- Instale la aplicación y todo el software en la nueva instancia.
- Restaure los datos.
- Si la instancia original tiene una dirección IP elástica y desea asegurarse de que los usuarios puedan continuar utilizando las aplicaciones de la nueva instancia de forma ininterrumpida, debe asociar la nueva instancia con la dirección IP elástica. Para obtener más información, consulte Direcciones IP elásticas.

Para cambiar el tipo de instancia para una nueva configuración de instancia

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. Haga una copia de seguridad de los datos que debe conservar, de la siguiente manera:

- Respecto de los datos en los volúmenes de almacén de instancia, realice una copia de seguridad de los datos en un almacenamiento persistente.
- Para datos en los volúmenes de EBS, cree una instantánea de los volúmenes o desconecte el volumen de la instancia para poder adjuntarlo a la nueva instancia más adelante.

3. En el panel de navegación, seleccione Instances (Instancia[s]).
4. Elija iniciar instancias. Cuando configure la instancia, haga lo siguiente:

   a. Seleccione una AMI que sea compatible con el tipo de instancia que desea. Tenga en cuenta que los tipos de instancia de generación actual requieren una AMI de HVM.
   b. Seleccione el nuevo tipo de instancia que desea. Si el tipo de instancia que desea no está disponible, eso significa que no es compatible con la configuración de la AMI que ha seleccionado.
   c. Si utiliza una dirección IP elástica, seleccione la VPC en la que se está ejecutando actualmente la instancia original.
   d. 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.
   e. Cuando haya terminado de configurar la nueva instancia, siga los pasos para seleccionar un par de claves y iniciar la instancia. Puede que transcurran unos minutos hasta que la instancia pase al estado `running`.

5. De ser necesario, adjunte los volúmenes de EBS basados en las instantáneas que ha creado, o cualquier volumen de EBS que haya desconectado de la instancia original, a la nueva instancia.
6. Instale la aplicación y todo el software necesario en la nueva instancia.
7. Realice un backup de los datos de los volúmenes de almacén de instancias de la instancia original.
8. Si utiliza una dirección IP elástica, asígnela a la instancia de la siguiente manera:

   a. En el panel de navegación, seleccione Elastic IPs (Direcciones IP elásticas).
   b. Seleccione la dirección IP elástica que está asociada a la instancia original y elija Actions (Acciones), Disassociate Elastic IP address (Desasociar dirección IP elástica). Cuando se le pida que confirme, elija Disassociate (Desasociar).
   c. Con la dirección IP elástica aún seleccionada, elija Actions (Acciones), Associate Elastic IP address (Asociar dirección IP elástica).
   d. En Tipo de recurso, seleccione Instancia.

e. En Instance (instancia), elija la nueva instancia con la que asociar la dirección IP elástica.

f. (Opcional) En Dirección IP privada, especifique una dirección IP privada a la que asociar la dirección IP elástica.

g. Elija Associate.

9. (Opcional) Puede terminar la instancia original si ya no la necesita. Seleccione la instancia y compruebe que esté a punto de terminar la instancia original, no la nueva (por ejemplo, compruebe el nombre o la hora de inicialización) y luego seleccione Estado de instancia, Cerrar instancia.

Compatibilidad para cambiar el tipo de instancia

Puede cambiar el tipo de instancia solo si el tipo de instancia que desea es compatible con la configuración actual de la instancia. Si el tipo de instancia que desea no es compatible con la configuración actual de la instancia, debe iniciar una nueva instancia con una configuración que sea compatible con el nuevo tipo de instancia que desea y, luego, migrar su aplicación a la nueva instancia.

[Instancias de Linux] Puede usar el manual de procedimientos de `AWSSupport-MigrateXenToNitroLinux` para migrar instancias compatibles de Linux de un tipo de instancia Xen a un tipo de instancia Nitro. Para obtener más información, consulte `AWSSupport-MigrateXenToNitroLinux runbook` en la Referencia del manual de procedimientos de automatización de AWS Systems Manager.

[Instancias de Windows] Para obtener más información sobre la migración de instancias de Windows compatibles de un tipo de instancia Xen a un tipo de instancia de Nitro, consulte Migrar a los tipos de instancias de última generación.

La compatibilidad se determina de las siguientes formas:

Tipo de virtualización

Las AMI de Linux utilizan uno de dos tipos de virtualización: paravirtual (PV) o máquina virtual de hardware (HVM). Si una instancia fue iniciada desde una AMI de PV, no puede cambiar a un tipo de instancia que solo sea HVM. Para obtener más información, consulte Tipos de virtualización de AMI. Para verificar el tipo de virtualización de la instancia, verifique el campo Virtualización en el panel de detalles de la pantalla Instancias de la consola de Amazon EC2.

Arquitectura

Las AMI son específicas para 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:

- Si el tipo de instancia actual tiene un procesador basado en la arquitectura Arm, se limita a los tipos de instancia que admiten un procesador basado en la arquitectura Arm, como C6g y M6g.
- 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 cambiar el tipo de instancia de una instancia de 32 bits, está limitado a estos tipos de instancia.

Adaptadores de red

Adaptadores de red: si cambia de un controlador para un adaptador de red a otro, la configuración del adaptador de red se restablece cuando el sistema operativo crea el nuevo adaptador. Para volver a establecer la configuración, es posible que necesite acceso a una cuenta local con permisos de administrador. A continuación, se muestran ejemplos de cómo pasar de un adaptador de red a otro:

- AWS PV (instancias T2) a Intel 82599 VF (instancias M4)
- Intel 82599 VF (la mayoría de las instancias M4) a ENA (instancias M5)
- ENA (instancias M5) a ENA de ancho de banda alto (instancias M5n)

Tarjetas de red

Algunos tipos de instancia admiten varias tarjetas de red. Debe seleccionar un tipo de instancia que admita la misma cantidad de tarjetas de red que el tipo de instancia actual.

Redes mejoradas

Los tipos de instancia que admiten redes mejoradas requieren que los controladores necesarios estén instalados. Por ejemplo, las instancias integradas en el AWS Nitro System requieren AMI respaldadas por EBS con los controladores Elastic Network Adapter (ENA) instalados. Para cambiar del tipo de instancia que no es compatible con redes mejoradas a un tipo que admita redes mejoradas, debe instalar los controladores de ENA o los controladores de ixgbevf en la instancia, según corresponda.

> **Note**
>
> Al cambiar el tamaño de una instancia con ENA Express activado, el nuevo tipo de instancia también debe ser compatible con ENA Express. Para ver una lista de los tipos

de instancias que admiten ENA Express, consulte Tipos de instancia compatibles con ENA Express.
Para hacer el cambio de un tipo de instancia que admite ENA Express a uno que no admite, asegúrese de que ENA Express no esté actualmente habilitada antes de cambiar el tamaño de la instancia.

NVMe

Los volúmenes de EBS se exponen como dispositivos de bloque NVMe en las instancias integradas en el AWS Nitro System. Si cambia desde 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 la asignación de dispositivos de bloques se cambian por los nombres de los dispositivos NVMe (`/dev/nvme[0-26]n1`).

[Instancias de Linux] 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.

Límites de volúmenes

La cantidad máxima de volúmenes de Amazon EBS que puede adjuntar a una instancia depende del tipo y tamaño de la instancia. Para obtener más información, consulte Límites de volumen de instancias.

Solo puede cambiar a un tipo o tamaño de instancia que admita el mismo número o mayor de volúmenes que los que están adjuntos actualmente a la instancia. Si cambia a un tipo o tamaño de instancia que no admite la cantidad de volúmenes adjuntos actualmente, se producirá un error en la solicitud. Por ejemplo, si cambia de una instancia `m7i.4xlarge` con 32 volúmenes adjuntos a una `m6i.4xlarge`, que admite un máximo de 27 volúmenes, se produce un error en la solicitud.

Solución de problemas de cambio del tipo de instancia

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que puedan surgir cuando cambia el tipo de instancia.

La instancia no se iniciará después de cambiar el tipo de instancia

Causa posible: no se cumplen los requisitos para el nuevo tipo de instancia

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 ¿Por qué no arranca una instancia de Linux después de cambiar su tipo?

Causa posible: la AMI no admite el tipo de instancia

Si utiliza la consola de EC2 para cambiar el tipo de instancia, solo están disponibles los tipos de instancia admitidos por la AMI seleccionada. No obstante, si utiliza la AWS CLI para iniciar una instancia, puede especificar una AMI y un tipo de instancia incompatibles. Si la AMI y el tipo de instancia son incompatibles, la instancia no se puede iniciar. Para obtener más información, consulte Compatibilidad para cambiar el tipo de instancia.

Causa posible: la instancia está en el grupo con ubicación en clúster

Si su instancia se encuentra en un grupo con ubicación en clúster y, después de cambiar el tipo de instancia, la instancia no se inicia, prueba lo siguiente:

1. Detenga todas las instancias del grupo con ubicación en clúster.
2. Cambie el tipo de instancia de la instancia afectada.
3. Inicie todas las instancias del grupo con ubicación en clúster.

No se puede acceder a la aplicación o el sitio web desde Internet después de cambiar el tipo de instancia

Posible causa: se publica la dirección IPv4 pública

Cuando se cambia el tipo de instancia, primero debe detener la instancia. Cuando detiene una instancia, liberamos la dirección IPv4 pública y le asignamos una nueva dirección IPv4 pública.

Para retener la dirección IPv4 pública entre las detenciones y los inicios de la instancia, le recomendamos que utilice una dirección IP elástica sin costo adicional siempre que la instancia se esté ejecutando. Para obtener más información, consulte Direcciones IP elásticas.

Cambiar el tipo de instancia de una instancia con respaldo en el almacén de instancias

Una instancia con respaldo en un almacén de instancias es una instancia que tiene un volumen raíz de almacén de instancias. No se puede cambiar el tipo de instancia de una instancia con volumen

raíz de almacén de instancia. En su lugar, debe crear una AMI a partir de la instancia, iniciar una nueva instancia desde esta AMI, seleccionar el tipo de instancia que desea y, a continuación, migrar la aplicación a la nueva instancia. Tenga en cuenta que el tipo de instancia que desea debe ser compatible con la AMI que cree. Para obtener información acerca de cómo se determina la compatibilidad, consulte Compatibilidad para cambiar el tipo de instancia.

Información general del proceso

- Haga una copia de seguridad de los datos de su instancia original.
- Cree una AMI a partir de la instancia original.
- Lance una nueva instancia desde esta AMI y seleccione el tipo de instancia que desea.
- Instale la aplicación en la nueva instancia.
- Si la instancia original tiene una dirección IP elástica y desea asegurarse de que los usuarios puedan continuar utilizando las aplicaciones de la nueva instancia de forma ininterrumpida, debe asociar la nueva instancia con la dirección IP elástica. Para obtener más información, consulte Direcciones IP elásticas.

Para cambiar el tipo de instancia de una instancia con respaldo en el almacén de instancias

1. Haga una copia de seguridad de los datos que debe conservar, de la siguiente manera:
   - Respecto de los datos en los volúmenes de almacén de instancia, realice una copia de seguridad de los datos en un almacenamiento persistente.
   - Para los datos de sus volúmenes de EBS, cree una instantánea de los volúmenes o separe el volumen de la instancia para poder adjuntarlo a la nueva instancia más adelante.
2. Cree una AMI desde la instancia cumpliendo los requisitos previos y siguiendo los procedimientos de Crear 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 en https://console.aws.amazon.com/ec2/.
4. En el panel de navegación, seleccione AMIs. En las listas de filtros, elija Owned by me (De mi propiedad) y la imagen que creó en el paso 2. 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.

> **Note**
>
> Si no ve la AMI que creó en el paso 2, compruebe que ha seleccionado la región en la que creó la AMI.

5. Con la AMI seleccionada, elija Launch instance from image (inicialización de instancias desde una imagen). Cuando configure la instancia, haga lo siguiente:

   a. Seleccione el nuevo tipo de instancia que desea. Si el tipo de instancia que desea no está disponible, eso significa que no es compatible con la configuración de la AMI que ha creado. Para obtener más información, consulte Compatibilidad para cambiar el tipo de instancia.

   b. Si utiliza una dirección IP elástica, seleccione la VPC en la que se está ejecutando actualmente la instancia original.

   c. 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.

   d. Cuando haya terminado de configurar la nueva instancia, siga los pasos para seleccionar un par de claves y iniciar la instancia. Puede que transcurran unos minutos hasta que la instancia pase al estado `running`.

6. De ser necesario, adjunte los volúmenes de EBS basados en las instantáneas que ha creado, o cualquier volumen de EBS que haya desconectado de la instancia original, a la nueva instancia.

7. Instale la aplicación y todo el software necesario en la nueva instancia.

8. Si utiliza una dirección IP elástica, asígnela a la instancia de la siguiente manera:

   a. En el panel de navegación, seleccione Elastic IPs (Direcciones IP elásticas).

   b. Seleccione la dirección IP elástica que está asociada a la instancia original y elija Actions (Acciones), Disassociate Elastic IP address (Desasociar dirección IP elástica). Cuando se le pida que confirme, elija Disassociate (Desasociar).

   c. Con la dirección IP elástica aún seleccionada, elija Actions (Acciones), Associate Elastic IP address (Asociar dirección IP elástica).

   d. En Tipo de recurso, seleccione Instancia.

   e. En Instance (instancia), elija la nueva instancia con la que asociar la dirección IP elástica.

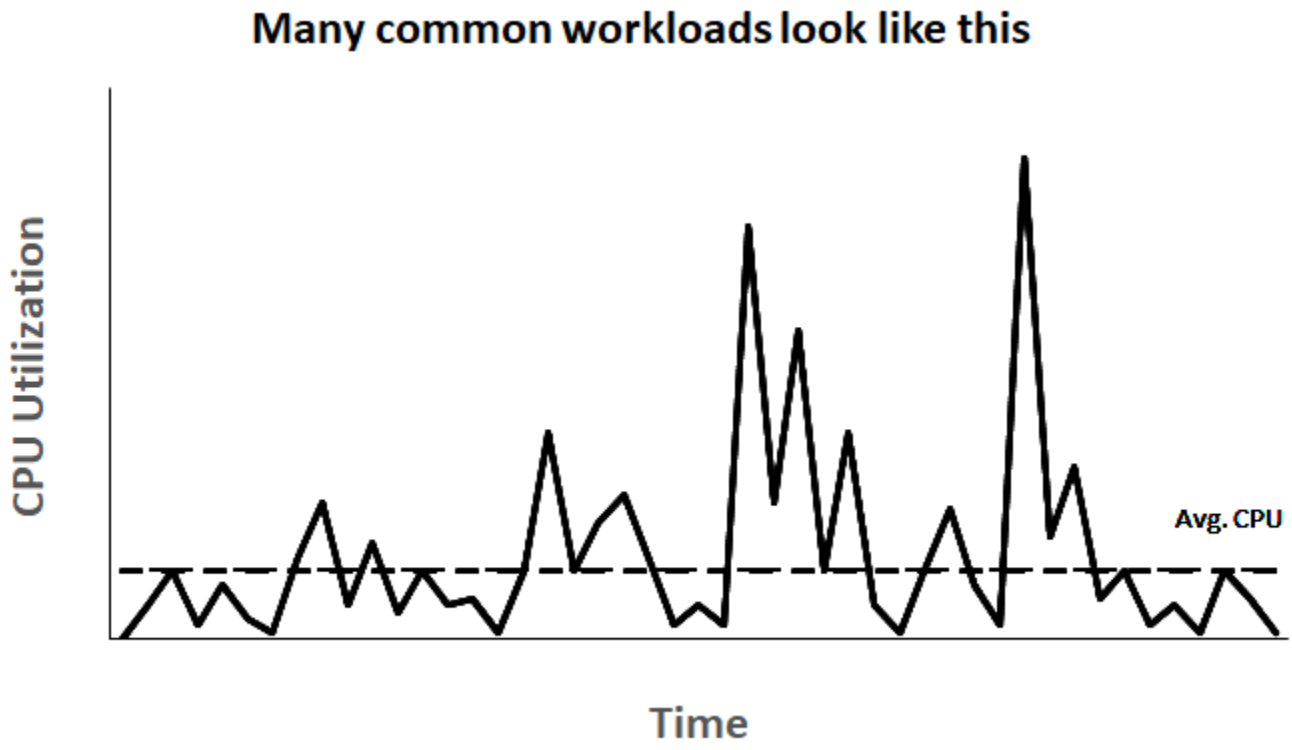
   f. (Opcional) En Dirección IP privada, especifique una dirección IP privada a la que asociar la dirección IP elástica.

   g. Elija Associate.

9. (Opcional) Puede terminar la instancia original si ya no la necesita. Seleccione la instancia y compruebe que esté a punto de terminar la instancia original, no la nueva (por ejemplo, compruebe el nombre o la hora de inicialización) y luego seleccione Estado de instancia, Cerrar instancia.

Instancias de rendimiento ampliable

En promedio, la mayoría de las cargas de trabajo de uso general no están ocupadas ni requieren un alto nivel de rendimiento sostenido de la CPU. En el siguiente gráfico, se ilustra la utilización de la CPU para muchas cargas de trabajo comunes que los clientes ejecutan en la nube de AWS en la actualidad.



Estas cargas de trabajo cuya utilización de la CPU es de baja a moderada conducen a un consumo excesivo de ciclos de vida de la CPU y, como resultado, se paga más de lo que se utiliza. Como solución, se pueden aprovechar las instancias de uso general ampliables y de bajo costo, que son las instancias T.

La familia de instancias T proporciona un rendimiento de base de referencia de la CPU con capacidad de ampliarse por encima del nivel de referencia en cualquier momento durante el tiempo que sea necesario. La CPU de referencia se define para satisfacer las necesidades de la mayoría

de las cargas de trabajo de uso general, incluidos los microservicios a gran escala, los servidores web, las bases de datos pequeñas y medianas, el registro de datos, los repositorios de código, los escritorios virtuales, los entornos de desarrollo y pruebas y las aplicaciones esenciales para el negocio. Las instancias T ofrecen un equilibrio de recursos de cómputo, memoria y red, y le proporcionan la manera más rentable de ejecutar un amplio espectro de aplicaciones de uso general que tienen un uso de la CPU de bajo a moderado. Pueden ahorrar hasta un 15 % en costos en comparación con las instancias M, y pueden generar aún más ahorros con tamaños de instancia más pequeños y económicos, que ofrecen hasta 2 vCPUs y 0,5 GiB de memoria. Los tamaños de instancia T más pequeños, como el nano, el micro, el pequeño y el mediano, son adecuados para cargas de trabajo que no requieren gran capacidad de memoria y no esperan un uso elevado de la CPU.

> **Note**
>
> En este tema se describe la CPU ampliable. Para obtener más información acerca del rendimiento de red ampliable, consulte Ancho de banda de red de instancias de Amazon EC2.

Tipos de instancias de EC2 ampliables

Las instancias de EC2 ampliables consisten en los tipos de instancias T4g, T3a y T3, así como a los correspondientes a la generación anterior T2.

Los tipos de instancias T4g son las instancias ampliables de última generación. Proporcionan la mejor relación precio-rendimiento, además del costo más bajo respecto a todos los tipos de instancias de EC2. Los tipos de instancia T4g están equipados con procesadores Graviton2 de AWS basados en ARM y cuentan con un amplio respaldo del ecosistema de proveedores de sistemas operativos, proveedores de software independientes y aplicaciones y servicios de AWS populares.

En la siguiente tabla, se resumen las principales diferencias entre los tipos de instancia ampliables.

Tipo	Descripción	Familia de procesadores
Última generación		
T4g	Tipo de instancia de EC2 de menor costo con una relación precio-rendimiento hasta un	Procesadores Graviton2 de AWS con núcleos Neoverse N1 de Arm

Tipo	Descripción	Familia de procesadores
	40 % superior y un costo 20 % menor en comparación con la T3	
T3a	instancias basadas en x86 de menor costo con un 10 % menos en comparación con las instancias T3	Procesadores EPYC de primera generación de AMD
T3	La mejor relación precio-rendimiento para cargas de trabajo x86 con hasta un 30 % menos en comparación con las instancias T2 de la generación anterior	Intel Xeon Scalable (procesadores Skylake, Cascade Lake)
Generación anterior		
T2	instancias ampliables de generaciones anteriores	Procesadores Intel Xeon

Para obtener información acerca del precio de la instancia y conocer especificaciones adicionales, consulte Precios de Amazon EC2 y Tipos de instancia de Amazon EC2. Para obtener más información acerca del rendimiento de red ampliable, consulte Ancho de banda de red de instancias de Amazon EC2.

Si su cuenta tiene menos de 12 meses de antigüedad, puede utilizar una instancia `t2.micro` de manera gratuita (o una instancia `t3.micro` en regiones en las que `t2.micro` no está disponible) con determinados límites de uso. Para obtener más información, consulte Capa gratuita de AWS.

Opciones de compra admitidas para instancias T

- On-Demand Instances
- Reserved Instances
- instancias dedicadas (únicamente T3)
- Hosts dedicados (únicamente T3, solo en modo `standard`)

- Spot Instances

Para obtener más información, consulte Opciones de compra de instancias.

Contenido

Prácticas recomendadas

Siga estas prácticas recomendadas para sacar el máximo beneficio de las instancias de rendimiento ampliable.

- Asegúrese de que el tamaño de la instancia que elija cumpla los requisitos de memoria mínimos del sistema operativo y las aplicaciones. Es posible que los sistemas operativos que tienen interfaces gráficas de usuario que consumen una cantidad importante de memoria y recursos de la CPU (por ejemplo, Windows) necesiten un tamaño de instancia de `t3.micro`, o incluso mayor, en muchos casos de uso. A medida que aumentan los requisitos de memoria y CPU de su carga de trabajo, dispone de la flexibilidad que ofrecen las instancias T para escalar a tamaños de instancia más grandes del mismo tipo o para seleccionar otro tipo de instancia.
- Habilite AWS Compute Optimizer para su cuenta y consulte las recomendaciones de Compute Optimizer para su carga de trabajo. Compute Optimizer puede ayudar a evaluar si las instancias deben aumentarse para mejorar el rendimiento o reducirse para ahorrar costos. Compute Optimizer también puede recomendar un tipo de instancia diferente según su situación. Para obtener más información, consulte Visualización de recomendaciones de instancias de EC2 en la Guía del usuario de AWS Compute Optimizer.

Conceptos clave y definiciones para las instancias de rendimiento ampliables

Los tipos de instancias de Amazon EC2 tradicionales proporcionan recursos de CPU fijos. Por otra parte, las instancias de rendimiento ampliable proporcionan un nivel de base de referencia de

utilización de la CPU con posibilidad de ampliarlo por encima de ese nivel de base de referencia. De este modo, se garantiza que solo pague la CPU de base de referencia más cualquier uso ampliado adicional de la CPU, con la consiguiente reducción de los costos de cómputo. La utilización de referencia y la capacidad de ampliar se rigen por créditos de CPU. Las instancias de rendimiento ampliable son los únicos tipos de instancia que usan créditos para el uso de la CPU.

Cada instancia de rendimiento ampliable obtiene continuamente créditos si se mantiene por debajo de la base de referencia de la CPU y también gasta créditos de manera continua si lo supera. La cantidad de créditos que se obtienen o se gastan depende de la utilización de la CPU de la instancia:

- Si la utilización de la CPU está por debajo de la base de referencia, los créditos que se obtienen son mayores que aquellos que se gastan.
- Si la utilización de la CPU coincide con la base de referencia, los créditos que se obtienen son iguales que aquellos que se gastan.
- Si la utilización de la CPU es mayor que la de la base de referencia, los créditos que se gastan son mayores que aquellos que se obtienen.

Cuando los créditos que se obtienen son mayores que los se gastan, entonces la diferencia se denomina créditos acumulados, que se pueden utilizar más adelante para ampliaciones por encima de la utilización de la CPU de base de referencia. Del mismo modo, cuando los créditos que se gastan son más que los que se obtienen, entonces el comportamiento de la instancia depende del modo de configuración de crédito: modo estándar o modo ilimitado.

En el modo estándar, cuando los créditos que se gastan son más que los que se obtienen, la instancia utiliza los créditos acumulados para ampliaciones por encima de la utilización de la CPU de base de referencia. Si no quedan créditos acumulados, la instancia se reduce gradualmente a la utilización de la CPU de base de referencia y no puede ampliarse por encima del nivel de base de referencia hasta tanto no acumule más créditos.

En el modo ilimitado, si la instancia se amplía por encima de la utilización de la CPU de base de referencia, la instancia utiliza en primer lugar los créditos acumulados para hacerlo. En caso de que no queden créditos acumulados, la instancia gasta los créditos sobrantes. Cuando el uso de la CPU cae por debajo de la base de referencia, utiliza los créditos de CPU que obtiene para compensar los créditos sobrantes gastados previamente. La posibilidad de obtener créditos de CPU para compensar créditos sobrantes permite a Amazon EC2 crear una media de utilización de la CPU de una instancia en un periodo de 24 horas. Si la utilización media de la CPU durante un periodo de 24

horas supera la base de referencia, se cobra el uso adicional de la instancia a una tarifa adicional fija por hora de vCPU.

Contenido

Conceptos y definiciones clave

Los siguientes conceptos y definiciones clave se pueden aplicar a las instancias de rendimiento ampliables.

Utilización de la CPU

> La utilización de la CPU es el porcentaje de unidades de cómputo de EC2 asignadas que están actualmente en uso en la instancia. Esta métrica mide el porcentaje de ciclos de la CPU asignados que se están utilizando en una instancia. La métrica de CloudWatch de utilización de la CPU muestra el uso de la CPU por instancia y no el uso por núcleo. La especificación de CPU de base de referencia de una instancia también se basa en el uso de CPU por instancia. Para medir la utilización de la CPU mediante la AWS Management Console o la AWS CLI, consulte Obtener estadísticas para una instancia específica.

Crédito de la CPU

> Una unidad de vCPU-time.
>
> Ejemplos:
>
> 1 crédito de CPU = 1 vCPU * 100 % de utilización x 1 minuto
>
> 1 crédito de CPU = 1 vCPU * 50 % de utilización x 2 minutos
>
> 1 crédito de CPU = 2 vCPU * 25 % de utilización x 2 minutos

Utilización de referencia

La utilización de referencia es el nivel en el que se puede utilizar la CPU para un saldo de crédito neto de cero, cuando el número de créditos de CPU que se gana coincide con el que se está utilizando. La utilización de referencia también se conoce como línea base. La utilización de base de referencia se expresa como un porcentaje de utilización de vCPU, que se calcula de la siguiente manera: utilización de base de referencia en % = (número de créditos obtenidos/número de vCPU)/60 minutos.

Para obtener información sobre la utilización básica de cada tipo de instancia de rendimiento con ráfagas, consulte la tabla de créditos.

Créditos obtenidos

Créditos obtenidos continuamente por una instancia mientras se está ejecutando.

Cantidad de créditos obtenidos por hora = % de utilización de base de referencia x cantidad de vCPUs x 60 minutos

Ejemplo:

Una instancia t3.nano con 2 vCPUs y una utilización de base de referencia del 5 % obtiene 6 créditos por hora, que se calculan de la siguiente manera:

2 vCPUs x 5 % de referencia x 60 minutos = 6 créditos por hora

Créditos gastados o utilizados

Créditos utilizados continuamente por una instancia mientras se está ejecutando.

Créditos de CPU que se gastan por minuto = número de vCPUs x utilización de la CPU x 1 minuto

Créditos acumulados

Créditos de CPU que no se han gastado cuando una instancia utiliza menos créditos de los necesarios para la utilización de base de referencia. En otras palabras, créditos acumulados = (créditos obtenidos - créditos utilizados) por debajo de la base de referencia.

Ejemplo:

Si un t3.nano se ejecuta a un 2 % de utilización de la CPU, que se sitúa por debajo de la referencia del 5 % durante una hora, los créditos acumulados se calculan de la siguiente manera:

Créditos de CPU acumulados = (créditos obtenidos por hora - créditos utilizados por hora) = 6 - 2 vCPUs x 2 % de utilización de la CPU x 60 minutos = 6 - 2,4 = 3,6 créditos acumulados por hora

Límite de acumulación de créditos

Depende del tamaño de la instancia, pero en general es igual al número máximo de créditos obtenidos en 24 horas.

Ejemplo:

Para t3.nano, el límite de acumulación de créditos = 24 x 6 = 144 créditos

Créditos de inicialización

Solo se aplica a las instancias T2 configuradas en modo estándar. Los créditos de inicialización constituyen una cantidad limitada de créditos de la CPU que se asignan a una nueva instancia T2 de manera tal que, al ser iniciada en modo estándar, pueda ampliarse por encima de la base de referencia.

Créditos sobrantes

Créditos que se gastan por una instancia una vez que se agota su saldo de crédito acumulado. Los créditos sobrantes están diseñados para que las instancias ampliables mantengan un alto rendimiento durante un periodo prolongado y solo se utilizan en el modo ilimitado. El saldo de créditos sobrantes se emplea para determinar cuántos créditos fueron utilizados por la instancia para la ampliación en modo ilimitado.

Modo estándar

Modo de configuración de créditos, que permite a una instancia ampliarse por encima de la base de referencia mediante el gasto de créditos que se han acumulado en el saldo correspondiente.

Modo ilimitado

Modo de configuración de créditos, que permite a una instancia ampliarse por encima de la base de referencia al mantener una utilización elevada de la CPU durante cualquier periodo siempre que sea necesario. El precio por hora de la instancia cubre automáticamente todos los picos de uso de la CPU si la utilización media de la CPU de una instancia CPU está a la par o por debajo de la base de referencia en un periodo de 24 horas o durante la vida útil de la instancia, lo que dure menos. Si la instancia requiere un mayor uso de la CPU durante un período prolongado, también puede hacerlo por un cargo fijo adicional por hora de vCPU.

En la siguiente tabla, se resumen las principales diferencias de créditos entre los tipos de instancia ampliables.

Tipo	Tipo de créditos de CPU admitidos	Modos de configuración de créditos	Vida útil de los créditos de la CPU acumulados entre los inicios y las detenciones de la instancia.
Última generación			
T4g	Créditos obtenidos, créditos acumulados, créditos gastados, créditos sobrantes (solo modo ilimitado)	Estándar, ilimitado (predeterminado)	7 días (los créditos se mantienen durante 7 días después de que se detiene una instancia)
T3a	Créditos obtenidos, créditos acumulados, créditos gastados, créditos sobrantes (solo modo ilimitado)	Estándar, ilimitado (predeterminado)	7 días (los créditos se mantienen durante 7 días después de que se detiene una instancia)
T3	Créditos obtenidos, créditos acumulados, créditos gastados, créditos sobrantes (solo modo ilimitado)	Estándar, ilimitado (predeterminado)	7 días (los créditos se mantienen durante 7 días después de que se detiene una instancia)
Generación anterior			
T2	Créditos obtenidos, créditos acumulados, créditos gastados, créditos de inicialización (solo modo estándar), créditos	Estándar (predeterminado), ilimitado	0 días (los créditos se pierden cuando se detiene una instancia)

Tipo	Tipo de créditos de CPU admitidos	Modos de configura ción de créditos	Vida útil de los créditos de la CPU acumulados entre los inicios y las detencion es de la instancia.
	sobrantes (solo modo ilimitado)		

> **Note**
>
> El modo ilimitado no es compatible con las instancias T3 que se inician en un host dedicado.

Ganar créditos de CPU

En función de su tamaño, cada instancia de rendimiento ampliable va adquiriendo continuamente (a una resolución de milisegundo) una tasa fija de créditos de CPU por hora. El proceso contable mediante el cual se determina si los créditos se acumulan o se gastan también se realiza a una resolución en el nivel de milisegundos, por lo que no tiene que preocuparse de gastar demasiados créditos de CPU; un pequeño aumento de la CPU solo utiliza una pequeña fracción de un crédito de CPU.

Si una instancia de rendimiento ampliable utiliza menos recursos de CPU que los requeridos para una utilización de referencia (por ejemplo cuando está inactiva), los créditos de CPU no gastados se acumulan en el saldo de créditos de CPU. Si una instancia de rendimiento ampliable tiene que ampliar por encima del nivel de utilización de referencia, gasta los créditos acumulados. Cuantos más créditos haya acumulado la instancia de rendimiento ampliable, más tiempo podrá ampliarse por encima de su nivel de utilización de la CPU cuando sea necesario.

En la siguiente tabla se indican los tipos de instancias de rendimiento ampliable, la tasa de adquisición de créditos por hora, el número máximo de créditos de CPU ganados que puede acumular una instancia, la cantidad de unidades vCPU por instancia y la utilización de referencia como porcentaje del núcleo total (al utilizar una sola vCPU).

Tipo de instancia	Créditos de CPU obtenidos por hora	Créditos máximos ganados que se pueden acumular*	vCPUs***	Utilización de referencia por vCPU
T2				
t2.nano	3	72	1	5%
t2.micro	6	144	1	10%
t2.small	12	288	1	20%
t2.medium	24	576	2	20 %**
t2.large	36	864	2	30 %**
t2.xlarge	54	1296	4	22,5 %**
t2.2xlarge	81.6	1958.4	8	17 %**
T3				
t3.nano	6	144	2	5 %**
t3.micro	12	288	2	10 %**
t3.small	24	576	2	20 %**
t3.medium	24	576	2	20 %**
t3.large	36	864	2	30 %**
t3.xlarge	96	2304	4	40 %**
t3.2xlarge	192	4608	8	40 %**
T3a				
t3a.nano	6	144	2	5 %**
t3a.micro	12	288	2	10 %**

Tipo de instancia	Créditos de CPU obtenidos por hora	Créditos máximos ganados que se pueden acumular*	vCPUs***	Utilización de referencia por vCPU
t3a.small	24	576	2	20 %**
t3a.medium	24	576	2	20 %**
t3a.large	36	864	2	30 %**
t3a.xlarge	96	2304	4	40 %**
t3a.2xlarge	192	4608	8	40 %**
T4g				
t4g.nano	6	144	2	5 %**
t4g.micro	12	288	2	10 %**
t4g.small	24	576	2	20 %**
t4g.medium	24	576	2	20 %**
t4g.large	36	864	2	30 %**
t4g.xlarge	96	2304	4	40 %**
t4g.2xlarge	192	4608	8	40 %**

* El número de créditos que se pueden acumular es equivalente a la cantidad de créditos que se pueden obtener en un periodo de 24 horas.

** La utilización de referencia de porcentaje en la tabla es por vCPU. En CloudWatch, el uso de la CPU se muestra por vCPU. Por ejemplo, el uso de la CPU de una instancia `t3.large` que funciona con el nivel de referencia se muestra como un 30 % en las métricas de CPU de

CloudWatch. Para obtener información acerca de cómo calcular la utilización de referencia, consulte Utilización de referencia.

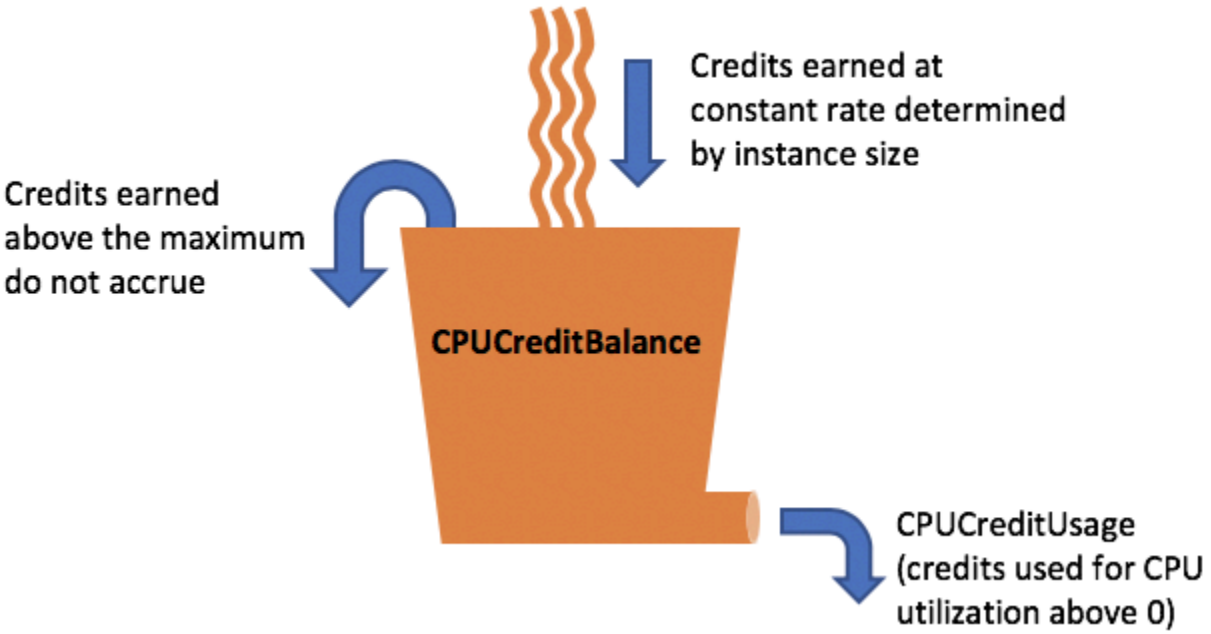
*** Cada vCPU es un subproceso de un núcleo Intel Xeon, o bien de un núcleo AMD EPYC, con excepción de las instancias T2 y T4g.

Tasa de obtención de créditos de CPU

El número de créditos de CPU obtenido por hora está determinado por el tamaño de la instancia. Por ejemplo, una `t3.nano` obtiene seis créditos por hora y una `t3.small`, 24 por hora. La tabla anterior enumera la tasa de obtención de créditos de todas las instancias.

Límite de acumulación de créditos de CPU

Aunque los créditos obtenidos no caducan nunca en una instancia en ejecución, hay un límite en cuanto al número de créditos obtenidos que una instancia puede acumular. El límite viene determinado por el límite de saldo de créditos de CPU. Una vez que se alcanza el límite, se descarta cualquier nuevo crédito obtenido, tal como se indica en la imagen siguiente. El bucket completo indica el límite de saldo de créditos de CPU y la capacidad superada indica los créditos recién obtenidos que superan el máximo.



El límite de saldo de créditos de CPU varía en función del tamaño de la instancia Por ejemplo, una instancia `t3.micro` puede acumular un saldo máximo de 288 créditos de CPU en el saldo de

créditos de CPU. La tabla anterior enumera la cantidad máxima de créditos obtenidos que puede acumular cada instancia.

Las instancias T2 Standard también adquieren créditos de inicialización. Los créditos de inicialización no cuentan para el límite de saldo de créditos de CPU. Si una instancia T2 no ha gastado sus créditos de inicialización y permanece inactiva durante un periodo de 24 horas mientras acumula créditos ganados, su saldo de créditos de CPU aparecerá por encima del límite. Para obtener más información, consulte Créditos de inicialización.

Las instancias T4g, T3a y T3 no obtienen créditos de inicialización. Estas instancias se inician como `unlimited` de forma predeterminada y, por tanto, se pueden ampliar inmediatamente tras iniciarse sin tener créditos de inicialización. Las instancias T3 iniciadas en un host dedicado se inician como `standard` de forma predeterminada; el modo `unlimited` no se admite para instancias T3 en un host dedicado.

Duración de los créditos de CPU acumulados

Los créditos de CPU de una instancia en ejecución no caducan.

Para T2, el saldo de créditos de CPU no persiste entre paradas e inicios de instancia. Si detiene una instancia T2, la instancia pierde todos sus créditos acumulados.

Para el caso de T4g, T3a y T3, el saldo de créditos de la CPU se mantiene durante siete días después de detenerse una instancia y, luego, se pierden. Si inicia la instancia en un plazo de siete días, no se pierde ningún crédito.

Para obtener más información, consulte `CPUCreditBalance` en la tabla de métricas de CloudWatch.

Utilización de referencia

La utilización de referencia es el nivel en el que se puede utilizar la CPU para un saldo de crédito neto de cero, cuando el número de créditos de CPU que se gana coincide con el que se está utilizando. La utilización de referencia también se conoce como línea base.

La utilización de referencia se expresa como un porcentaje de la utilización de la vCPU, que se calcula de la siguiente manera:

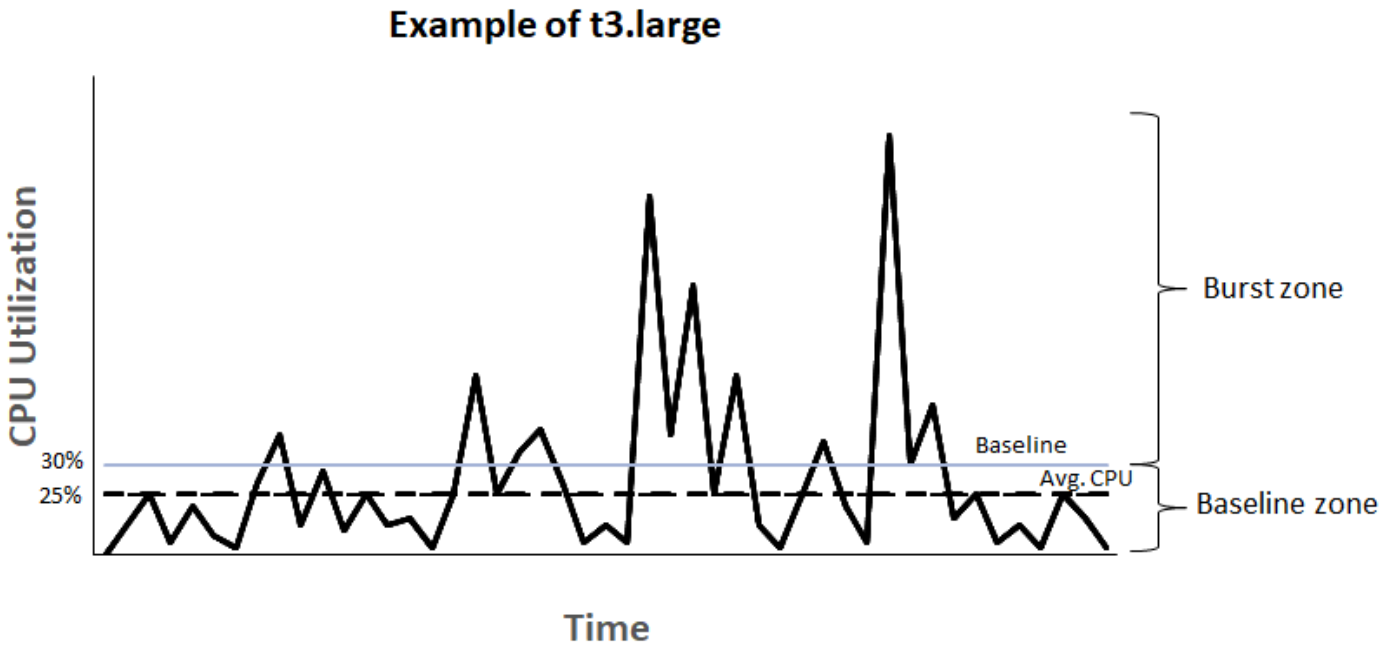
```
(number of credits earned/number of vCPUs)/60 minutes = % baseline
utilization
```

Por ejemplo, una instancia `t3.nano`, con 2 vCPU, obtiene 6 créditos por hora, lo que genera una utilización de referencia del 5 %, que se calcula de la siguiente manera:

```
(6 credits earned/2 vCPUs)/60 minutes = 5% baseline utilization
```

Una instancia `t3.large`, con 2 vCPU, obtiene 36 créditos por hora, lo que genera una utilización de línea de base del 30 % (`(36/2)/60`).

En el siguiente gráfico, se proporciona un ejemplo de una instancia `t3.large` con una utilización promedio de la CPU por debajo de la línea de base.



Modo ilimitado para las instancias de rendimiento ampliable

Una instancia de rendimiento ampliable configurada como `unlimited` puede sostener una utilización de la CPU alto durante cualquier periodo siempre que sea necesario. El precio por hora de la instancia cubre automáticamente todos los picos de uso de la CPU si la utilización media de la CPU de una instancia CPU está a la par o por debajo de la base de referencia en un periodo de 24 horas o durante la vida útil de la instancia, lo que dure menos.

Para la gran mayoría de las cargas de trabajo de uso general, las instancias configuradas como `unlimited` proporcionan una rentabilidad suficiente sin cargos adicionales. Si la instancia requiere un mayor uso de la CPU durante un período prolongado, también puede hacerlo por un cargo fijo adicional por hora de vCPU. Para obtener información acerca de los precios, consulte Precios de Amazon EC2 y Precios de instancias T2/T3/T4 en modo ilimitado.

Si utiliza una instancia `t2.micro` o `t3.micro` con la oferta de Nivel gratuito de AWS y lo hace en el modo `unlimited`, podrían aplicarse cargos si la utilización promedio en un periodo de 24 horas supera la utilización de base de referencia de la instancia.

Las instancias T4g, T3a y T3 se inician como `unlimited` de forma predeterminada (a menos que cambie la opción predeterminada). Si el uso medio de CPU durante un período de 24 horas supera la base de referencia, incurre en cargos por créditos excedentes. Si inicia instancias de spot como `unlimited` y planea usarlas inmediatamente y durante un corto período de tiempo, sin tiempo de inactividad para acumular créditos de CPU, incurre en cargos por créditos excedentes. Le recomendamos iniciar sus instancias de spot en modo estándar para evitar pagar costos más elevados. Para obtener más información, consulte Los créditos sobrantes pueden generar costos y Instancias de rendimiento ampliable.

> **Note**
>
> Las instancias T3 iniciadas en un host dedicado se inician como `standard` de forma predeterminada; el modo `unlimited` no se admite para instancias T3 en un host dedicado.

Contenido

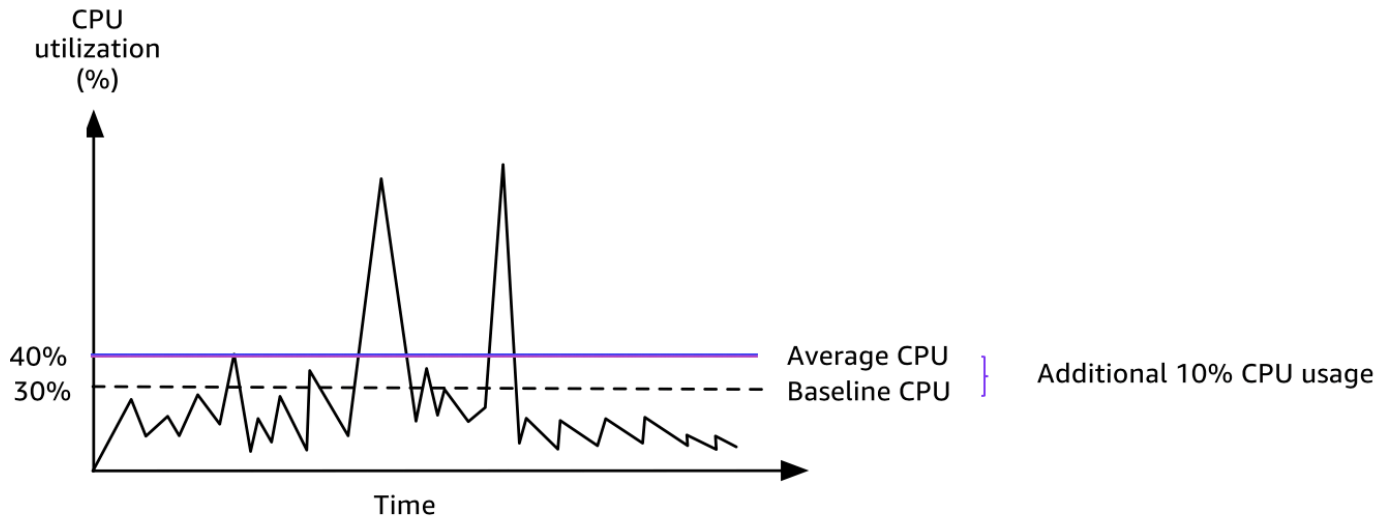
Sobre el modo ilimitado

El modo `unlimited` es una opción de configuración de créditos para instancias de rendimiento ampliable. Se puede habilitar y deshabilitar en cualquier momento para una instancia en ejecución o que esté detenida. Puede configurar `unlimited` como opción de crédito predeterminada de las cuentas por región de AWS y por familia de instancias de rendimiento ampliable, de modo que todas las nuevas instancias de rendimiento ampliable de la cuenta se lancen mediante la opción de crédito predeterminada.

Cómo funcionan las instancias de rendimiento ampliable ilimitado

Si una instancia de rendimiento ampliable configurada como `unlimited` agota los créditos que ha acumulado en su saldo de créditos de CPU, puede gastar créditos sobrantes para ampliar por encima de la referencia. Cuando el uso de la CPU cae por debajo de la base de referencia, utiliza los créditos de CPU que obtiene para compensar los créditos sobrantes gastados previamente. La posibilidad de obtener créditos de CPU para compensar créditos sobrantes permite a Amazon EC2 crear una media de utilización de la CPU de una instancia en un periodo de 24 horas. Si la utilización media de la CPU durante un periodo de 24 horas supera la base de referencia, se cobra el uso adicional de la instancia a una tarifa adicional fija por hora de vCPU.

En el gráfico siguiente se muestra el uso de CPU de una instancia `t3.large`. La utilización de CPU de referencia de una instancia `t3.large` es del 30%. Si la instancia se ejecuta con un 30% de utilización de la CPU o menos de media durante un periodo de 24 horas, no se realizará ningún cargo adicional porque el costo ya está cubierto por el precio por hora de la instancia. Sin embargo, si la instancia se ejecuta con un 40 % de utilización de la CPU de media durante un periodo de 24 horas, como se muestra en el gráfico, se cobra el 10 % de uso de CPU adicional de la instancia a una tarifa adicional fija por hora de vCPU.



Para obtener más información sobre la utilización de referencia por vCPU para cada tipo de instancia y cuántos créditos obtiene cada tipo de instancia, consulte la tabla de créditos.

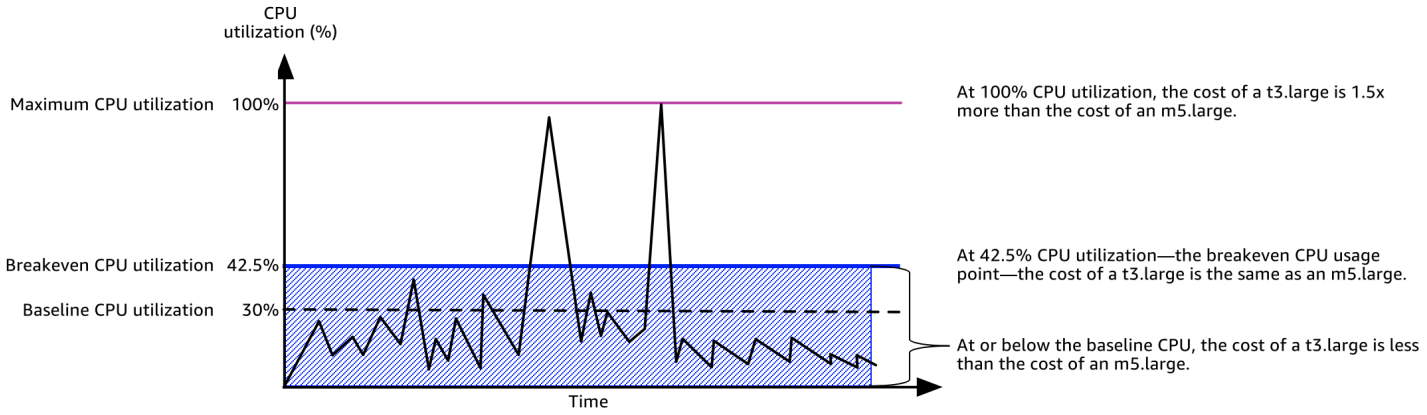
Cuando utilizar el modo ilimitado en lugar del modo de CPU fija

A la hora de determinar si debería utilizar una instancia de rendimiento ampliado en el modo `unlimited`, como una instancia T3, o una instancia de rendimiento fijo, como una instancia M5, debe determinar el límite de rentabilidad de uso de CPU. El límite de rentabilidad de uso de CPU para una instancia de rendimiento ampliable es el punto en que una instancia de rendimiento ampliable cuesta lo mismo que una instancia de rendimiento fijo. El límite de rentabilidad de uso de CPU le ayuda a determinar lo siguiente:

- Si el uso medio de CPU durante un periodo de 24 horas está a la par o por debajo del límite de rentabilidad de uso de CPU, utilice una instancia de rendimiento ampliable en el modo `unlimited` para poder beneficiarse del precio menor de una instancia de rendimiento ampliable y obtener el mismo rendimiento que con una instancia de rendimiento fijo.
- Si el uso medio de CPU durante un periodo de 24 horas es superior al límite de rentabilidad de uso de CPU, la instancia de rendimiento ampliable le costará más que una instancia de rendimiento fijo de tamaño equivalente. Si una instancia T3 consume continuamente el 100% de la CPU, acabará pagando aproximadamente 1,5 veces el precio de una instancia M5 de tamaño equivalente.

En el siguiente gráfico se muestra el límite de rentabilidad de uso de CPU donde una instancia `t3.large` cuesta lo mismo que una instancia `m5.large`. El límite de rentabilidad de uso de CPU de una instancia `t3.large` es el 42,5%. Si el uso medio de CPU es del 42,5%, el costo de ejecutar la

instancia `t3.large` es el mismo que el de una instancia `m5.large` y más caro si el uso medio de CPU es superior al 42,5%. Si la carga de trabajo necesita menos del 42,5 % de uso medio de CPU, puede beneficiarse del precio menor de la instancia `t3.large` y conseguir el mismo rendimiento que con una instancia `m5.large`.



En la tabla siguiente se muestra cómo calcular el límite de rentabilidad de uso de CPU para que pueda determinar cuándo es más barato utilizar una instancia de rendimiento ampliable en modo `unlimited` o una instancia de rendimiento fijo. Las columnas de la tabla abarcan de la A a la K.

Tipo de instancia	vCPU	Precio de T3*/ hora	Precio de M5*/ hora	Diferencia de precio	Utilización de referencia T3 por vCPU (%)	Cargo por hora de vCPU de créditos sobrantes	Cargo por minuto de vCPU	Minutos adicionales disponibles por vCPU	% de CPU adicional disponible	Límite de rentabilidad de CPU (%)
A	B	C	D	E = D - C	F	G	H = G / 60	I = E / H	J = (I / 60) / B	K = F + J
t3.large	2	0,0835 USD	0,096 USD	0,0125 US	30%	0,05 USD	0,000833 US	15	12,5%	42,5%

* Precio basado en us-east-1 y sistema operativo Linux.

La tabla proporciona la siguiente información:

- La columna A muestra el tipo de instancia, `t3.large`.
- La columna B muestra la cantidad de vCPU de la instancia `t3.large`.
- La columna C muestra el precio de una instancia `t3.large` por hora.
- La columna D muestra el precio de una instancia `m5.large` por hora.
- La columna E muestra la diferencia de precio entre la instancia `t3.large` y la instancia `m5.large`.
- La columna F muestra la utilización de referencia por vCPU de la instancia `t3.large`, que es el 30 %. Con el nivel de referencia, el costo por hora de la instancia cubre el costo de uso de la CPU.
- La columna G muestra la tarifa adicional fija por hora de vCPU que se cobra a una instancia si consume el 100 % de la CPU una vez que ha consumido los créditos obtenidos.
- La columna H muestra la tarifa adicional fija por minuto de vCPU que se cobra a una instancia si consume el 100 % de la CPU una vez que ha consumido los créditos obtenidos
- La columna I muestra el número de minutos adicionales que la instancia `t3.large` puede ejecutarse por hora usando el 100% de la CPU y pagando el mismo precio por hora que una instancia `m5.large`.
- La columna J muestra el uso de CPU adicional (en %) con respecto al valor de referencia que puede consumir la instancia pagando el mismo precio por hora que una instancia `m5.large`.
- La columna K muestra el límite de rentabilidad de uso de la CPU (en %) de la instancia `t3.large` sin pagar más que con la instancia `m5.large`. Si el valor es superior a este, la instancia `t3.large` costará más que la instancia `m5.large`.

En la tabla siguiente se muestra el límite de rentabilidad de uso de la CPU (en %) para tipos de instancias T3 comparado con tipos de instancias M5 de tamaño similar.

Tipo de instancia T3	Límite de rentabilidad de uso de la CPU (en %) para T3 comparado con M5
`t3.large`	42,5%
`t3.xlarge`	52,5%
`t3.2xlarge`	52,5%

Los créditos sobrantes pueden generar costos

Si la utilización media de la CPU de una instancia está a la par o por debajo del nivel de referencia, no se incurre en gastos adicionales. Como una instancia obtiene la cantidad máxima de créditos en un periodo de 24 horas (por ejemplo, una instancia `t3.micro` puede obtener hasta 288 créditos en un periodo de 24 horas), puede gastar créditos sobrantes hasta esa cantidad máxima sin que se realicen cargos inmediatamente.

Sin embargo, si el uso de la CPU se mantiene por encima de la base de referencia, la instancia no puede obtener créditos suficientes para compensar los créditos sobrantes que ha gastado. Los créditos sobrantes que no se han compensado se cobran a una tarifa plana adicional por hora de vCPU. Para obtener información acerca de la tarifa, consulte Precios de instancias T2/T3/T4g en modo ilimitado.

Los créditos sobrantes que se gastaron anteriormente se cobran cuando se da alguno de los casos siguientes:

- Los créditos sobrantes gastados superan el número máximo de créditos que la instancia puede obtener en un periodo de 24 horas. Los créditos sobrantes gastados por encima de la cantidad máxima se cobran al final de la hora.
- La instancia se detiene o se termina.
- La instancia se cambia de `unlimited` a `standard`.

La métrica `CPUSurplusCreditBalance` de CloudWatch hace el seguimiento de los créditos sobrantes gastados. La métrica `CPUSurplusCreditsCharged` de CloudWatch hace el seguimiento de los créditos sobrantes. Para obtener más información, consulte Métricas de CloudWatch adicionales para las instancias de rendimiento ampliable.

Ausencia de créditos de inicialización para instancias T2 ilimitadas

Las instancias T2 Standard reciben créditos de inicialización, pero las instancias T2 Unlimited no. Las instancias T2 Unlimited pueden realizar ráfagas por encima de la base de referencia en cualquier momento sin cargos adicionales, siempre y cuando la utilización media de la CPU esté a la par o por debajo de la base de referencia a lo largo de un periodo de 24 horas o durante la vida útil de la instancia, lo que dure menos. Como tal, las instancias T2 Unlimited no requieren créditos de inicialización para alcanzar un alto rendimiento inmediatamente después de la inicialización.

Si una instancia T2 se cambia de `standard` a `unlimited`, los créditos de inicialización acumulados se eliminan de `CPUCreditBalance` antes de trasladar el `CPUCreditBalance` restante.

Las instancias T4g, T3a y T3 nunca reciben créditos de inicialización debido a que admiten el modo ilimitado. La configuración de crédito de modo ilimitado permite a las instancias T4g, T3a y T3 utilizar tanta CPU como sea necesario para ampliarse por encima de la base de referencia y durante el tiempo que sea necesario.

Habilitar el modo ilimitado

Puede pasar de `unlimited` a `standard` y de `standard` a `unlimited` en cualquier momento, en una instancia en ejecución o que esté detenida. Para obtener más información, consulte Para iniciar una instancia de rendimiento ampliable como ilimitada o estándar y Modificación de la especificación de crédito de una instancia de rendimiento ampliable.

Puede configurar `unlimited` como opción de crédito predeterminada en el nivel de cuenta por región de AWS y por familia de instancias de rendimiento ampliable, de modo que todas las nuevas instancias de rendimiento ampliable de la cuenta se lancen mediante la opción de crédito predeterminada. Para obtener más información, consulte Configuración de la especificación de crédito predeterminada para la cuenta.

Puede verificar si la instancia de rendimiento ampliable está configurada como `unlimited` o `standard` con la consola de Amazon EC2 o con la AWS CLI. Para obtener más información, consulte Ver la especificación de crédito de una instancia de rendimiento ampliable y Consulta de la especificación de crédito predeterminada.

Qué ocurre con los créditos al cambiar entre ilimitadas y estándar

`CPUCreditBalance` es una métrica de CloudWatch que hace un seguimiento del número de créditos que ha acumulado una instancia. `CPUSurplusCreditBalance` es una métrica de CloudWatch que hace un seguimiento del número de créditos sobrantes que ha gastado una instancia.

Cuando cambia una instancia configurada como `unlimited` a `standard`, se produce la siguiente situación:

- El valor de `CPUCreditBalance` permanece sin cambios y se traspasa.
- El valor de `CPUSurplusCreditBalance` se cobra de inmediato.

Cuando una instancia `standard` se cambia a `unlimited`, se produce la siguiente situación:

- El valor de `CPUCreditBalance` que contiene los créditos obtenidos acumulados se traspasa.

- En el caso de instancias T2 Standard, los créditos de inicialización se eliminan del valor de `CPUCreditBalance` y se traspasa el valor de `CPUCreditBalance` restante con los créditos obtenidos acumulados.

Supervisar el uso de crédito

Para saber si la instancia está gastando más créditos de lo que proporciona la base de referencia, puede utilizar las métricas de CloudWatch para realizar un seguimiento de ese uso y configurar alarmas por hora para recibir notificaciones al respecto. Para obtener más información, consulte Supervisión de los créditos de su CPU en busca de instancias de rendimiento ampliable.

Ejemplos de modo ilimitado

En los siguientes ejemplos se explica el uso de créditos para las instancias configuradas como `unlimited`.

Ejemplos

- Ejemplo 1: Explicación del uso de crédito con T3 ilimitadas
- Ejemplo 2: Explicación del uso de crédito con T2 ilimitadas

Ejemplo 1: Explicación del uso de crédito con T3 ilimitadas

En este ejemplo, puede ver el uso de la CPU de una instancia `t3.nano` iniciada como `unlimited` y cómo gasta los créditos obtenidos y sobrantes para mantener la utilización de la CPU.

Una instancia `t3.nano` obtiene 144 créditos de CPU en un periodo de 24 horas, que puede canjear 144 minutos de uso de la vCPU. Cuando se agota el saldo de créditos de CPU (representado por la métrica CloudWatch de `CPUCreditBalance`), puede gastar créditos de CPU sobrantes que—aún no ha obtenido —para realizar ráfagas durante el tiempo que sea necesario. Como una instancia `t3.nano` obtiene la cantidad máxima de 144 créditos en un periodo de 24 horas, puede gastar créditos sobrantes hasta esa cantidad máxima sin que se realicen cargos inmediatamente. Si gasta más de 144 créditos de CPU, se cobra la diferencia al terminar la hora.

La intención del ejemplo, ilustrado en el gráfico de abajo, es mostrar cómo una instancia puede realizar ráfagas con créditos sobrantes incluso después de haber agotado el `CPUCreditBalance`. El siguiente flujo de trabajo hace referencia a los puntos numerados en el gráfico:

P1 – en la hora 0 en el gráfico, la instancia se inicia como `unlimited` y comienza a obtener créditos inmediatamente. La instancia permanece inactiva desde el momento de su inicialización, (el uso

de la CPU es 0%) y no se gasta ningún crédito. Todos los créditos no gastados se acumulan en el saldo de créditos. Durante las primeras 24 horas: `CPUCreditUsage` está a 0 y el valor de `CPUCreditBalance` llega a su máximo de 144.

P2 – durante las siguientes 12 horas, el uso de la CPU está en un 2,5 %, por debajo de la base de referencia del 5 %. La instancia obtiene más créditos de los que gasta, pero el valor de `CPUCreditBalance` no puede sobrepasar su máximo de 144 créditos.

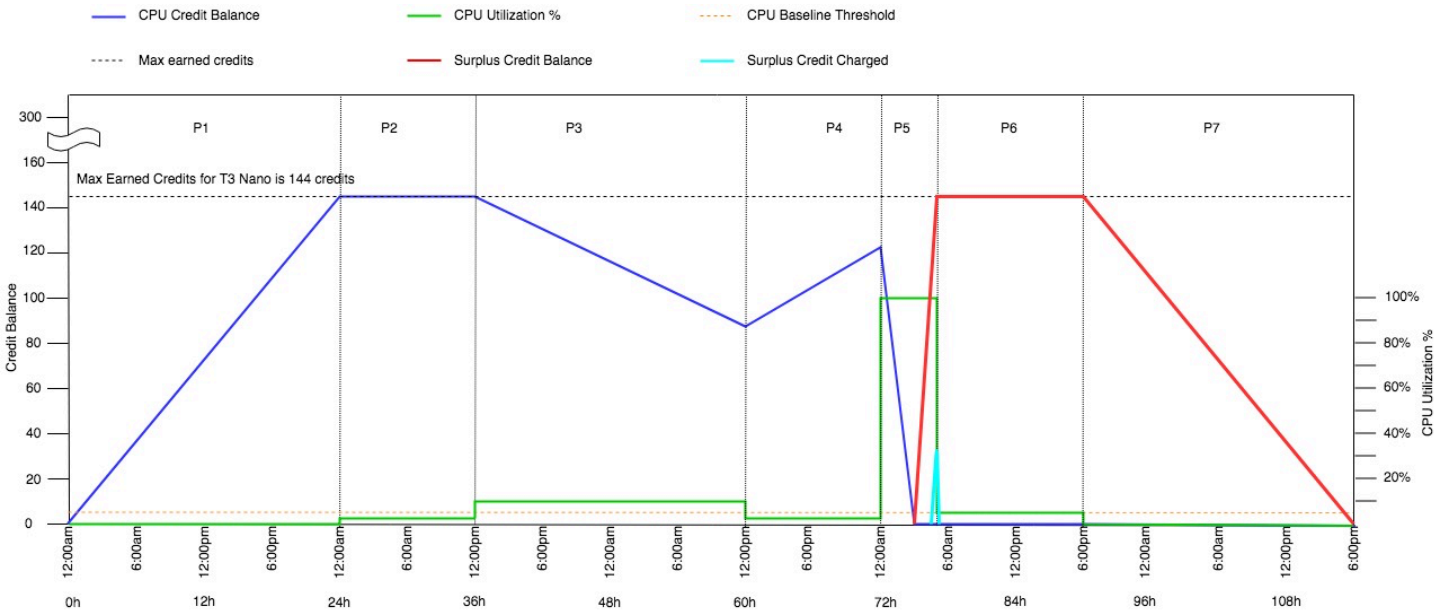
P3: – durante las 24 horas siguientes, el uso de la CPU está en un 7 % (por encima de la base de referencia), lo cual requiere un gasto de 57,6 créditos. La instancia gasta más créditos de los que obtiene y el valor de `CPUCreditBalance` se reduce a 86,4 créditos.

P4: – durante las siguientes 12 horas, el uso de la CPU disminuye al 2,5 % (por debajo de la base de referencia), lo cual requiere un gasto de 36 créditos. Al mismo tiempo, la instancia obtiene 72 créditos. La instancia obtiene más créditos de los que gasta y el valor de `CPUCreditBalance` aumenta a 122 créditos.

P5 – durante las siguientes 5 horas, la instancia se amplía al 100 % del uso de la CPU y gasta un total de 570 créditos para sostener la ampliación. Alrededor de una hora después de iniciarse este periodo, la instancia agota su saldo `CPUCreditBalance` total de 122 créditos, y comienza a gastar créditos sobrantes para mantener una alta utilización de la CPU, lo que suma 448 créditos sobrantes en este periodo (570-122 = 448). Cuando el valor de `CPUSurplusCreditBalance` alcanza los 144 créditos de CPU (el máximo que una instancia `t3.nano` puede obtener en un periodo de 24 horas), los créditos sobrantes gastados a partir de ese momento no se podrán compensar con los créditos obtenidos. Los créditos sobrantes gastados posteriormente ascienden a 304 créditos (448-144=304), lo que implica un pequeño cargo adicional al final de la hora por 304 créditos.

P6: – durante las siguientes 13 horas, el uso de la CPU es de un 5 % (la base de referencia). La instancia obtiene tantos créditos como gasta, sin exceso para contribuir al saldo `CPUSurplusCreditBalance`. El valor de `CPUSurplusCreditBalance` se mantiene en 144 créditos.

P7 – durante las últimas 24 horas de este ejemplo, la instancia permanece inactiva y el uso de la CPU es del 0 %. Durante este tiempo, la instancia obtiene 144 créditos, los cuales utiliza para el saldo `CPUSurplusCreditBalance`.



Ejemplo 2: Explicación del uso de crédito con T2 ilimitadas

En este ejemplo, puede ver el uso de la CPU de una instancia `t2.nano` iniciada como `unlimited` y cómo gasta los créditos obtenidos y sobrantes para mantener la utilización de la CPU.

Una instancia `t2.nano` obtiene 72 créditos de CPU en un periodo de 24 horas, que puede canjear 72 minutos de uso de la vCPU. Cuando se agota el saldo de créditos de CPU (representado por la métrica CloudWatch de `CPUCreditBalance`), puede gastar créditos de CPU sobrantes que— aún no ha obtenido —para realizar ráfagas durante el tiempo que sea necesario. Como una instancia obtiene la cantidad `t2.nano` de 72 créditos en un periodo de 24 horas, puede gastar créditos sobrantes hasta esa cantidad máxima sin que se realicen cargos inmediatamente. Si gasta más de 72 créditos de CPU, se cobra la diferencia al terminar la hora.

La intención del ejemplo, ilustrado en el gráfico de abajo, es mostrar cómo una instancia puede realizar ráfagas con créditos sobrantes incluso después de haber agotado el `CPUCreditBalance`. Puede suponer que al inicio de la línea temporal que se muestra en el gráfico, la instancia tiene un saldo de crédito acumulado igual al número máximo de créditos que puede ganar en 24 horas. El siguiente flujo de trabajo hace referencia a los puntos numerados en el gráfico:

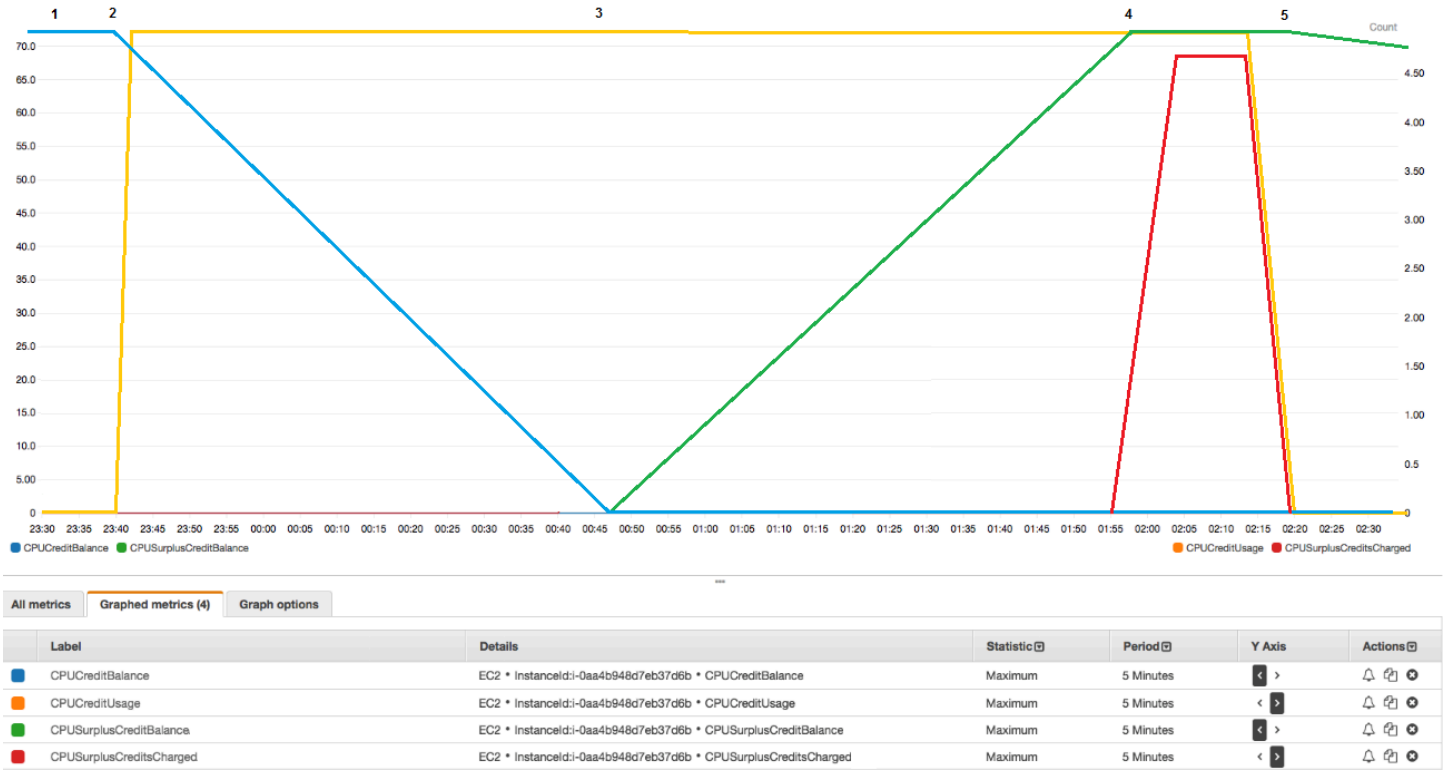
1 – en los primeros 10 minutos, `CPUCreditUsage` está a 0 y el valor de `CPUCreditBalance` se mantiene en el máximo de 72.

2: – a las 23:40, a medida que el uso de la CPU aumenta, la instancia gasta créditos de CPU y el valor de `CPUCreditBalance` disminuye.

3: – cerca de las 00:47, la instancia agota todo el crédito de `CPUCreditBalance` y comienza a gastar los créditos sobrantes para mantener la alta utilización de la CPU.

4 – los créditos sobrantes se gastan hasta las 01:55, cuando el valor de `CPUSurplusCreditBalance` alcanza los 72 créditos de CPU. Esto equivale a la cantidad máxima que puede obtener una instancia `t2.nano` en un periodo de 24 horas. Los créditos sobrantes gastados posteriormente no se pueden compensar con los créditos obtenidos en el periodo de 24 horas, lo que implica un pequeño cargo adicional al final de la hora.

5 – la instancia continúa gastando créditos sobrantes hasta aproximadamente las 02:20. En este momento, la utilización de la CPU cae por debajo de la base de referencia y la instancia comienza a obtener 3 créditos por hora (o 0,25 créditos cada 5 minutos), que utiliza para compensar el `CPUSurplusCreditBalance`. Una vez que el valor de `CPUSurplusCreditBalance` llega a 0, la instancia comienza a acumular créditos ganados en su `CPUCreditBalance` a una velocidad de 0,25 créditos cada 5 minutos.



Calcular la factura (instancia de Linux)

Los créditos sobrantes cuestan 0,05 USD por hora de vCPU. La instancia ha gastado aproximadamente 25 créditos sobrantes entre la 01:55 y las 02:20, que equivale a 0,42 horas de vCPU. Los cargos adicionales para esta instancia son de 0,42 horas de vCPU por 0,05 USD/hora

de vCPU, que equivale a 0,021 USD, redondeado a 0,02 USD. Esta es la factura de fin de mes para esta instancia de T2 Unlimited:

Amazon Elastic Compute Cloud running Linux/UNIX		
$0.0058 per On Demand Linux t2.nano Instance Hour	720.000 Hrs	$4.18

Amazon Elastic Compute Cloud T2 CPU Credits		
$0.05 per vCPU-Hour of T2 CPU credits	0.420 vCPU-Hours	$0.02

Calcular la factura (instancia de Windows)

Los créditos sobrantes cuestan 0,096 USD por hora de vCPU. La instancia ha gastado aproximadamente 25 créditos sobrantes entre la 01:55 y las 02:20, que equivale a 0,42 horas de vCPU. Los cargos adicionales para esta instancia son de 0,42 horas de vCPU por 0,096 USD/hora de vCPU, que equivale a 0,04032 USD, redondeado a 0,04 USD. Esta es la factura de fin de mes para esta instancia de T2 Unlimited:

Amazon Elastic Compute Cloud running Windows		
$0.0081 per On Demand Windows t2.nano Instance Hour	720.000 Hrs	$5.83

Amazon Elastic Compute Cloud T2 CPU Credits		
$0.096 per vCPU-Hour of T2 CPU credits	0.420 vCPU-Hours	$0.04

Puede crear alertas de facturación para recibir notificaciones cada hora acerca de los cargos acumulados y poder tomar medidas en caso necesario.

Modo estándar para las instancias de rendimiento ampliable

Las instancias de rendimiento ampliable configuradas como `standard` son adecuadas para cargas de trabajo con un uso de la CPU medio situado siempre por debajo de la utilización de la CPU de referencia de la instancia. Para ampliar por encima de la base de referencia, la instancia gasta créditos que ha acumulado en su saldo de créditos de CPU. Si la instancia se está quedando sin créditos acumulados, la utilización de la CPU se reduce gradualmente hasta el nivel de referencia, para que no experimente un descenso brusco del rendimiento cuando se quede sin créditos de CPU acumulados en su saldo. Para obtener más información, consulte Conceptos clave y definiciones para las instancias de rendimiento ampliables.

Contenido

Sobre el modo estándar

El modo `standard` es una opción de configuración para instancias de rendimiento ampliable. Se puede habilitar y deshabilitar en cualquier momento para una instancia en ejecución o que esté detenida. Puede configurar `standard` como opción de crédito predeterminada de las cuentas por región de AWS y por familia de instancias de rendimiento ampliable, de modo que todas las nuevas instancias de rendimiento ampliable de la cuenta se lancen mediante la opción de crédito predeterminada.

Cómo funcionan las instancias de rendimiento ampliable estándar

Cuando una instancia de rendimiento ampliable configurada como `standard` está en estado de ejecución, obtiene continuamente (a una resolución de milisegundo) una proporción fija de créditos por hora. Cuando se detiene una instancia T2 Standard, pierde todos los créditos acumulados y se pone a cero su balance de créditos. Cuando se reinicia, recibe un nuevo conjunto de créditos de inicialización y empieza a cumular créditos acumulados. Para las instancias T4g, T3a y T3 estándar, el saldo de créditos de la CPU se mantiene durante siete días una vez que se detiene una instancia y, luego, se pierden. Si inicia la instancia en un plazo de siete días, no se pierde ningún crédito.

Las instancias T2 estándar reciben dos tipos de créditos de CPU: créditos obtenidos y créditos de inicialización. Cuando una instancia T2 Standard está en estado de ejecución, obtiene continuamente (a una resolución en el nivel de milisegundo) una proporción fija de créditos obtenidos por hora. Al iniciarse, aún no tiene créditos obtenidos para una buena experiencia de startup; por tanto, para proporcionar una buena experiencia de startup, al iniciar recibe créditos de inicialización, que gasta inicialmente mientras acumula créditos obtenidos.

Las instancias T4g, T3a y T3 no reciben créditos de inicialización debido a que admiten el modo ilimitado. La configuración de crédito de modo ilimitado permite a las instancias T4g, T3a y T3 utilizar tanta CPU como sea necesario para ampliarse por encima de la base de referencia y durante el tiempo que sea necesario.

Créditos de inicialización

En el momento de la inicialización o al iniciarse, las instancias T2 Standard obtienen 30 créditos de inicialización por vCPU, y las instancias T1 Standard obtienen 15 créditos de inicialización. Por ejemplo, una instancia `t2.micro` tiene una vCPU y obtiene 30 créditos de inicialización y una instancia `t2.xlarge` tiene cuatro vCPU y obtiene 120. Los créditos de inicialización están diseñados para ofrecer una buena experiencia de startup para permitir a las instancias realizar ráfagas inmediatamente después de la inicialización, antes de que hayan acumulado créditos obtenidos.

Los créditos de inicialización se gastan en primer lugar, antes que los créditos obtenidos. Los créditos de inicialización que no se gastan se acumulan en el saldo de créditos de CPU, pero no cuentan para el límite de saldo de créditos de CPU. Por ejemplo, una instancia `t2.micro` tiene un límite de saldo de créditos de CPU de 144 créditos ganados. Si se ha iniciado y ha permanecido inactiva durante más de 24 horas, su saldo de créditos de CPU alcanza 174 (30 créditos de inicialización + 144 créditos obtenidos), que está por encima del límite. Sin embargo, después de que la instancia gaste los 30 créditos de inicialización, el saldo de créditos no podrá volver a superar los 144. Para obtener más información acerca del límite de saldo de créditos de la CPU obtenidos en función del tamaño de cada instancia, consulte la tabla de créditos.

La siguiente tabla enumera la adjudicación inicial de créditos de CPU recibidos en el momento de inicialización o comienzo, y la cantidad de vCPU.

Tipo de instancia	Créditos de inicialización	vCPU
`t1.micro`	15	1

Tipo de instancia	Créditos de inicialización	vCPU
t2.nano	30	1
t2.micro	30	1
t2.small	30	1
t2.medium	60	2
t2.large	60	2
t2.xlarge	120	4
t2.2xlarge	240	8

Límites de créditos de inicialización

Hay un límite en el número de veces que las instancias T2 Standard pueden recibir créditos de inicialización. El límite predeterminado es de 100 inicializacións o comienzos de todas las instancias T2 Standard combinados por cuenta, por región, durante un periodo de 24 horas. Por ejemplo, el límite se alcanza cuando se detiene una instancia y se inicia 100 veces en un período de 24 horas o cuando se inician 100 instancias dentro de un período de 24 horas u otras combinaciones que equivalen a 100 inicios. Es posible que las cuentas nuevas tengan un límite inferior que aumenta con el tiempo según el uso que le dé.

> **Tip**
>
> Para asegurarse de que sus cargas de trabajo siempre contarán con el rendimiento que requieren, cambie a Modo ilimitado para las instancias de rendimiento ampliable o considere la posibilidad de usar una instancia mayor.

Diferencias entre créditos de inicialización y créditos obtenidos

En la siguiente tabla se enumeran las diferencias entre los créditos de inicialización y los créditos obtenidos.

	Créditos de inicialización	Créditos obtenidos
Tasa de obtención de créditos	En el momento de la inicialización o al iniciarse, las instancias T2 Standard obtienen 30 créditos de inicialización por vCPU. Si la instancia T2 cambia de `unlimited` a `standard`, no obtiene créditos de inicialización en el momento del cambio.	En función de su tamaño, cada instancia T2 gana continuamente (a una resolución en el nivel de milisegundo) una proporción fija de créditos de CPU por hora. Para obtener más información acerca del número de créditos de la CPU obtenidos por tamaño de instancia, consulte la tabla de créditos.
Límite de obtención de créditos	El límite para recibir créditos de inicialización es de 100 inicializacións o inicios de todas las instancias T2 Standard combinadas por cuenta, por región, durante un periodo de 24 horas. Es posible que las cuentas nuevas tengan un límite inferior que aumenta con el tiempo según el uso que le dé.	Una instancia T2 no puede acumular más créditos que el límite de saldo de crédito de CPU. Si el saldo de créditos de CPU ha llegado a su límite, se descarta cualquier crédito obtenido después de haber alcanzado el límite. Los créditos de inicialización no cuentan para el límite. Para obtener más información acerca del límite de saldo de créditos de la CPU obtenidos en función del tamaño de la instancia T2, consulte la tabla de créditos.
Uso de créditos	Los créditos de inicialización se gastan en primer lugar, antes que los créditos obtenidos.	Los créditos obtenidos solo se gastan después de agotar todos los créditos de inicialización.
Vencimiento de créditos	Cuando una instancia T2 Standard está en ejecución, los créditos de inicialización no caducan. Cuando una instancia T2 Standard se detiene o cambia a T2 Unlimited, se pierden todos los créditos de inicialización.	Cuando una instancia T2 está en ejecución, los créditos que se han acumulado no caducan. Cuando se detiene la instancia T2, todos los créditos acumulados obtenidos se pierden.

El seguimiento del número de créditos de inicialización acumulados y créditos obtenidos acumulados se realiza mediante la métrica de CloudWatch `CPUCreditBalance`. Para obtener más información, consulte `CPUCreditBalance` en la tabla de métricas de CloudWatch.

Ejemplos de modo estándar

En los siguientes ejemplos se explica el uso de créditos cuando las instancias se configuran como `standard`.

Ejemplos

- Ejemplo 1: Explicación del uso del crédito con T3 estándar
- Ejemplo 2: Explicación del uso del crédito con T2 estándar

Ejemplo 1: Explicación del uso del crédito con T3 estándar

En este ejemplo, puede ver cómo una instancia `t3.nano` iniciada como `standard` obtiene, acumula y gasta créditos obtenidos. Vea cómo el saldo de créditos refleja los créditos obtenidos acumulados.

Una instancia `t3.nano` en ejecución obtiene 144 créditos cada 24 horas. Su límite de saldo de créditos es 144 créditos obtenidos. Una vez que se ha alcanzado el límite, cualquier nuevo crédito que se gane se descarta. Para obtener más información acerca del número de créditos que se pueden obtener y acumular, consulte la tabla de créditos.

Puede iniciar una instancia T3 Standard y utilizarla inmediatamente. O puede iniciar una instancia T3 Standard y dejarla inactiva durante unos días antes de ejecutar aplicaciones en ella. El número de créditos acumulados o gastados dependerá de si una instancia se usa o permanece inactiva. Si una instancia permanece inactiva durante 24 horas desde el momento en que se ha iniciado, el saldo de créditos alcanza su límite, que es el número máximo de créditos obtenidos acumulados que se puede acumular.

En este ejemplo, se describe una instancia que permanece inactiva durante 24 horas a partir del momento en que se ha iniciado, y se le guía paso a paso por siete periodos de tiempo a lo largo de un periodo de 96 horas, mostrando la frecuencia a la que se obtienen, acumulan, gastan y descartan los créditos, así como el valor del saldo de créditos al final de cada periodo.

El siguiente flujo de trabajo hace referencia a los puntos numerados en el gráfico:

P1 – en la hora 0 en el gráfico, la instancia se inicia como `standard` y comienza a obtener créditos inmediatamente. La instancia permanece inactiva desde el momento de su inicialización, (el uso

de la CPU es 0%) y no se gasta ningún crédito. Todos los créditos no gastados se acumulan en el saldo de créditos. Durante las primeras 24 horas: `CPUCreditUsage` está a 0 y el valor de `CPUCreditBalance` llega a su máximo de 144.

P2 – durante las siguientes 12 horas, el uso de la CPU está en un 2,5 %, por debajo de la base de referencia del 5 %. La instancia obtiene más créditos de los que gasta, pero el valor de `CPUCreditBalance` no puede sobrepasar su máximo de 144 créditos. Los créditos obtenidos por encima del límite se descartan.

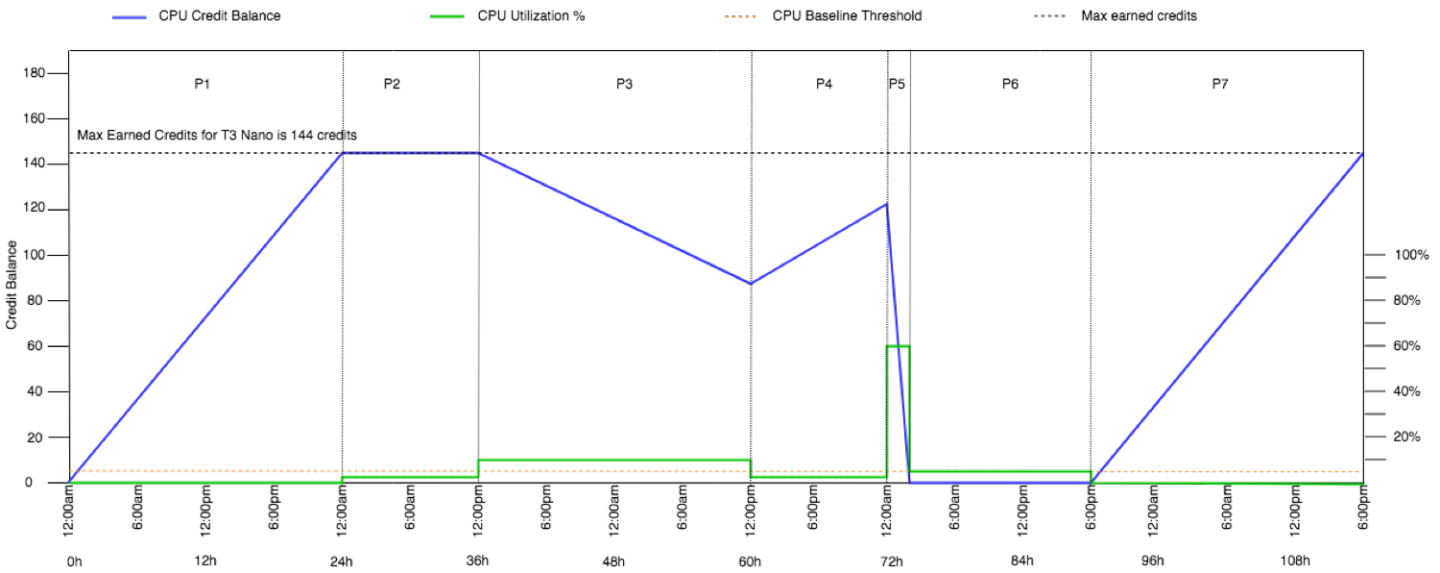
P3: – durante las 24 horas siguientes, el uso de la CPU está en un 7 % (por encima de la base de referencia), lo cual requiere un gasto de 57,6 créditos. La instancia gasta más créditos de los que obtiene y el valor de `CPUCreditBalance` se reduce a 86,4 créditos.

P4: – durante las siguientes 12 horas, el uso de la CPU disminuye al 2,5 % (por debajo de la base de referencia), lo cual requiere un gasto de 36 créditos. Al mismo tiempo, la instancia obtiene 72 créditos. La instancia obtiene más créditos de los que gasta y el valor de `CPUCreditBalance` aumenta a 122 créditos.

P5: durante las dos horas siguientes, la instancia se amplía al 60 % del uso de la CPU y gasta todo el valor de `CPUCreditBalance` de 122 créditos. Al final de este periodo, con `CPUCreditBalance` a cero, se fuerza a bajar el uso de la CPU al nivel de utilización de referencia del 5 %. Durante el uso de la base de referencia, la instancia obtiene tantos créditos como gasta.

P6: – durante las 14 horas siguientes, el uso de la CPU es de un 5 % (la base de referencia). La instancia adquiere tantos créditos como gasta. El valor de `CPUCreditBalance` se mantiene en 0 créditos.

P7 – durante las últimas 24 horas de este ejemplo, la instancia permanece inactiva y el uso de la CPU es del 0 %. Durante este tiempo, la instancia adquiere 144 créditos, que se acumula en su saldo `CPUCreditBalance`.



Ejemplo 2: Explicación del uso del crédito con T2 estándar

En este ejemplo, puede ver cómo una instancia `t2.nano` iniciada como `standard` obtiene, acumula y gasta créditos obtenidos y de inicialización. Verá cómo el saldo de créditos refleja no solo los créditos obtenidos acumulados, sino también los créditos de inicialización acumulados.

Una instancia `t2.nano` obtiene 30 créditos de inicialización cuando se inicia y 72 créditos cada 24 horas. El límite de su saldo de créditos es de 72 créditos obtenidos; los créditos de inicialización no cuentan para este límite. Una vez que se ha alcanzado el límite, cualquier nuevo crédito que se gane se descarta. Para obtener más información acerca del número de créditos que se pueden obtener y acumular, consulte la tabla de créditos. Para obtener más información acerca de los límites, consulte Límites de créditos de inicialización.

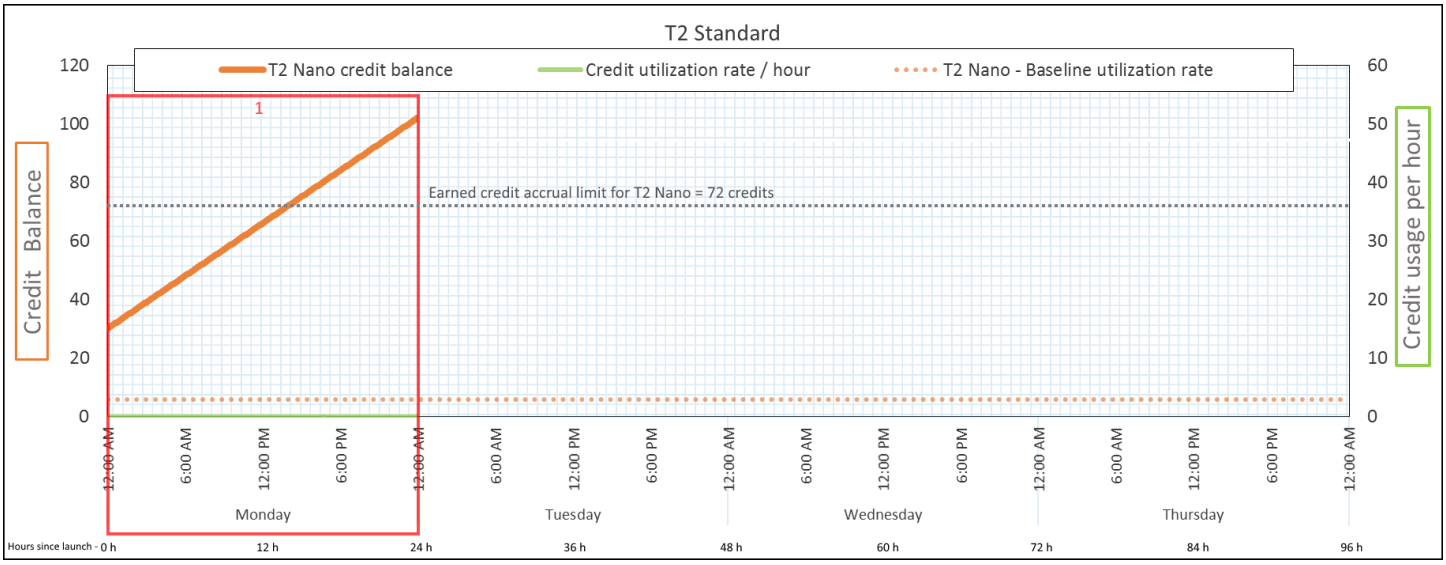
Puede iniciar una instancia T2 Standard y utilizarla inmediatamente. O puede iniciar una instancia T2 Standard y dejarla inactiva durante unos días antes de ejecutar aplicaciones en ella. El número de créditos acumulados o gastados dependerá de si una instancia se usa o permanece inactiva. Si una instancia permanece inactiva durante 24 horas desde el momento en que se ha iniciado, el saldo de créditos aparecerá por encima del límite debido a que el saldo refleja tanto los créditos obtenidos acumulados como los créditos de inicialización acumulados. Sin embargo, una vez que se usa la CPU, los créditos de inicialización se gastan en primer lugar. A partir de ese momento, el límite siempre refleja la cantidad máxima de créditos obtenidos que se pueden acumular.

En este ejemplo, se describe una instancia que permanece inactiva durante 24 horas a partir del momento en que se ha iniciado, y se le guía paso a paso por siete periodos de tiempo a lo largo de

un periodo de 96 horas, mostrando la frecuencia a la que se obtienen, acumulan, gastan y descartan los créditos, así como el valor del saldo de créditos al final de cada periodo.

Periodo 1: 1 – 24 horas

En la hora 0 en el gráfico, la instancia T2 se inicia como `standard` y obtiene inmediatamente 30 créditos de inicialización. La instancia sigue obteniendo créditos mientras está en el estado de ejecución. La instancia permanece inactiva desde el momento de su inicialización, (el uso de la CPU es 0%) y no se gasta ningún crédito. Todos los créditos no gastados se acumulan en el saldo de créditos. Aproximadamente 14 horas después de la inicialización, el saldo de créditos es de 72 (30 créditos de inicialización + 42 créditos obtenidos), que es el equivalente a lo que la instancia puede obtener en 24 horas. 24 horas después de la inicialización, el saldo de créditos supera los 72 créditos, puesto que los créditos de inicialización no gastados se acumulan— en el saldo de créditos (el saldo de créditos es de 102 créditos: 30 créditos de inicialización + 72 créditos obtenidos).



Tasa de gasto de créditos	0 créditos cada 24 horas (0% de uso de la CPU)
Tasa de obtención de créditos	72 créditos cada 24 horas
Tasa de descarte de créditos	0 créditos cada 24 horas
Saldo de créditos	102 créditos (30 créditos de inicialización + 72 créditos obtenidos)

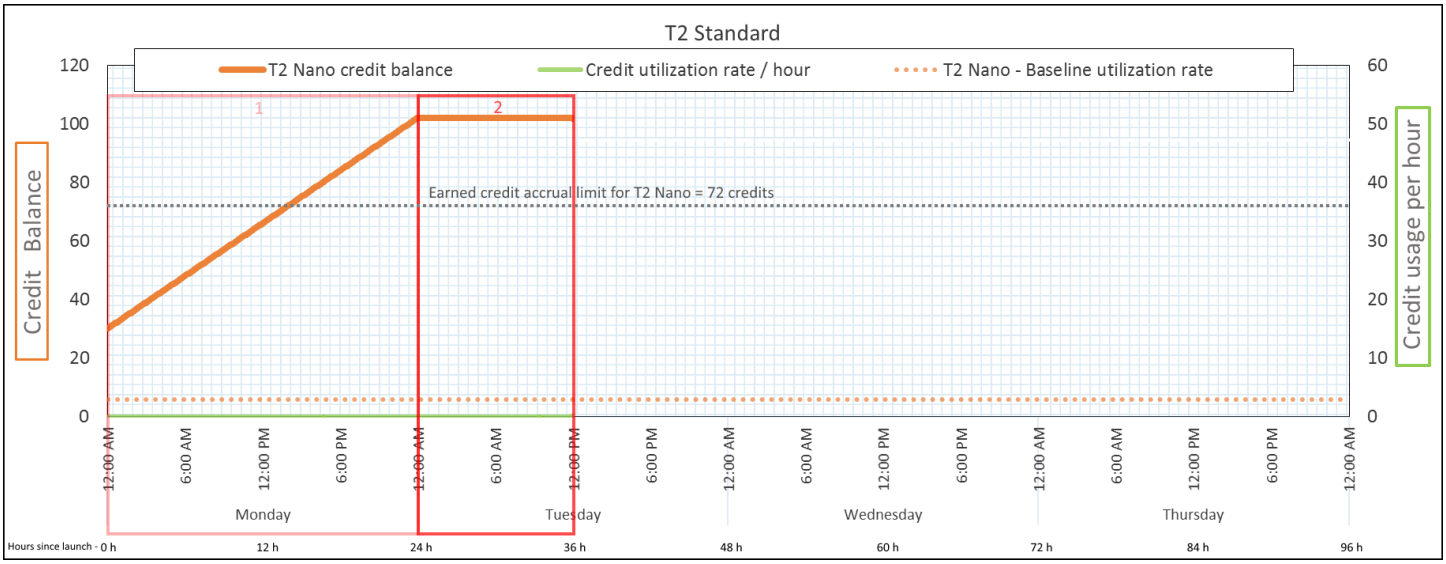
Conclusión

Si no hay uso de la CPU después de la inicialización, la instancia acumula más créditos de los que puede obtener en 24 horas (30 créditos de inicialización + 72 créditos obtenidos = 102 créditos).

En una situación real, una instancia de EC2 consume una pequeña cantidad de créditos mientras se inicia y ejecuta, lo que impide que el saldo alcance el valor máximo teórico de este ejemplo.

Periodo 2: 25 – 36 horas

Durante las siguientes 12 horas, la instancia sigue inactiva y continúa obteniendo créditos, pero el saldo de créditos no aumenta. Se detiene en 102 créditos (30 créditos de inicialización + 72 créditos obtenidos). El saldo de créditos ha llegado a su límite de 72 créditos obtenidos acumulados, por lo que se descartan los créditos recién obtenidos.



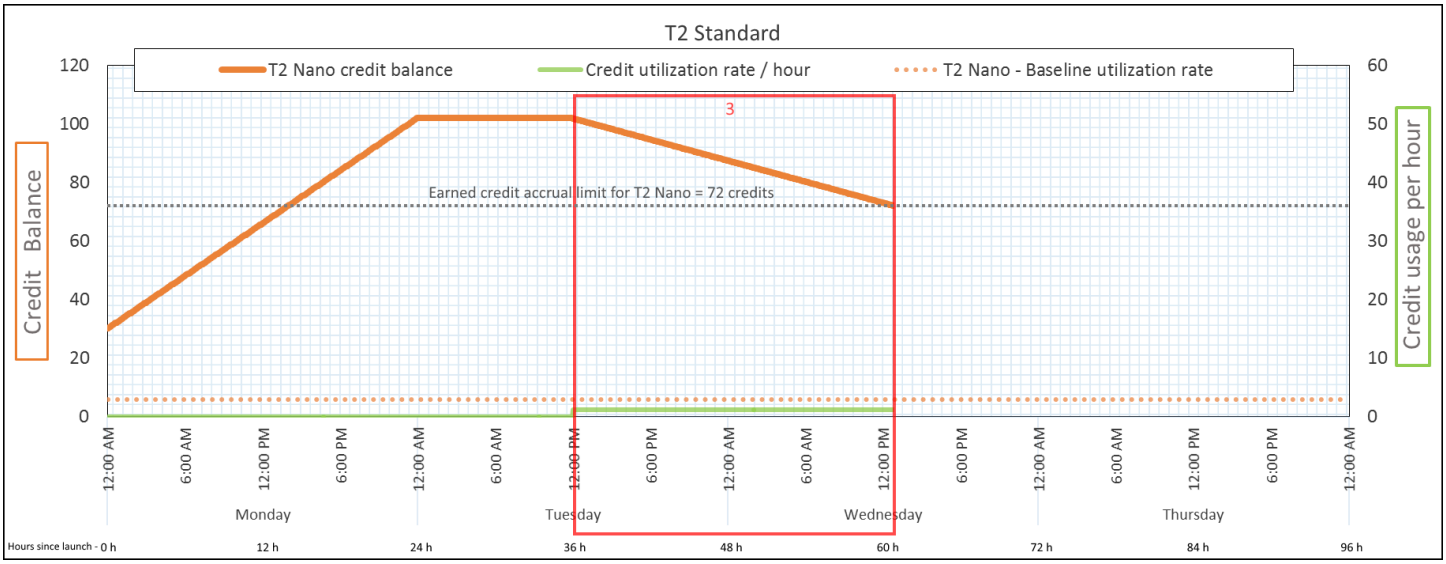
Tasa de gasto de créditos	0 créditos cada 24 horas (0% de uso de la CPU)
Tasa de obtención de créditos	72 créditos cada 24 horas (3 créditos por hora)
Tasa de descarte de créditos	72 créditos cada 24 horas (100% de tasa de obtención de créditos)
Saldo de créditos	102 créditos (30 créditos de inicialización + 72 créditos obtenidos) — el saldo no cambia.

Conclusión

Una instancia obtiene créditos constantemente, pero no puede acumular más créditos obtenidos si el saldo de créditos ha alcanzado su límite. Una vez que se ha alcanzado el límite, cualquier nuevo crédito que se obtenga se descarta. Los créditos de inicialización no cuentan para el límite de saldo de créditos. Si el saldo incluye los créditos de inicialización acumulados, aparecerá por encima del límite.

Periodo 3: 37 – 61 horas

Durante las siguientes 25 horas, la instancia utiliza el 2% de la CPU, lo que requiere 30 créditos. En el mismo periodo, obtiene 75 créditos, pero el saldo de créditos disminuye. El saldo disminuye porque los créditos de inicialización acumulados se gastan en primer lugar, mientras que los créditos recién obtenidos se descartan debido a que el saldo de créditos ha alcanzado el límite de 72 créditos obtenidos.



Tasa de gasto de créditos	28,8 créditos cada 24 horas (1,2 créditos por hora, 2% de uso de la CPU, 40% de tasa de obtención de créditos): 30— créditos en 25 horas
Tasa de obtención de créditos	72 créditos cada 24 horas
Tasa de descarte de créditos	72 créditos cada 24 horas (100% de tasa de obtención de créditos)

Saldo de créditos	72 créditos (30 créditos de inicialización gastados; 72 créditos obtenidos sin gastar)

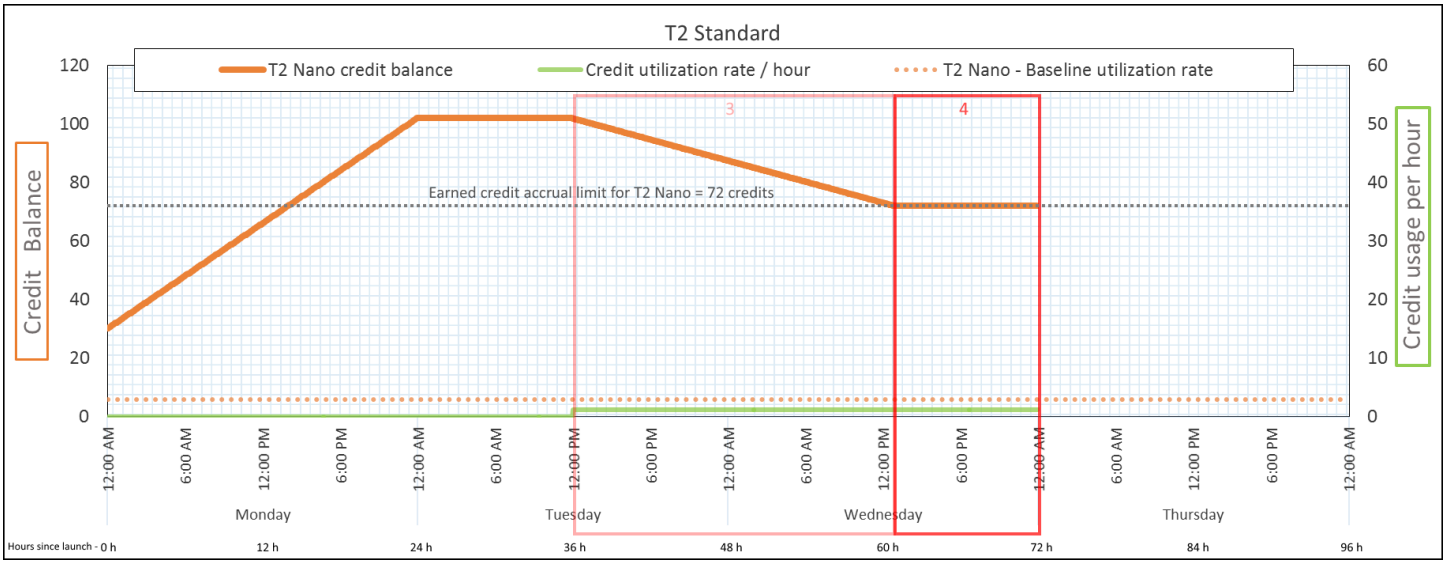
Conclusión

Una instancia gasta los créditos de inicialización antes que los créditos obtenidos. Los créditos de inicialización no cuentan para el límite de créditos. Una vez que se han gastado los créditos de inicialización, el saldo nunca podrá superar lo que se puede obtener en 24 horas. Además, una instancia que se está ejecutando no puede obtener más créditos de inicialización.

Periodo 4: 62 – 72 horas

Durante las siguientes 11 horas, la instancia utiliza el 2% de la CPU, lo que requiere 13.2 créditos. Este es el mismo uso de la CPU que el del periodo anterior, pero el saldo no disminuye. Permanece en 72 créditos.

El saldo no disminuye porque la tasa de obtención de créditos es superior a la tasa de gasto de créditos. En el intervalo en el que la instancia gasta 13,2 créditos, también obtiene 33. Sin embargo, el límite del saldo es de 72 créditos, por lo que se descartarán todos los créditos obtenidos que superen dicho límite. El saldo se detiene en 72 créditos, no en 102 créditos como ocurre en el periodo 2, ya que no hay créditos de inicialización acumulados.



Tasa de gasto de créditos	28,8 créditos cada 24 horas (1,2 créditos por hora, 2% de uso de la CPU, 40% de tasa de

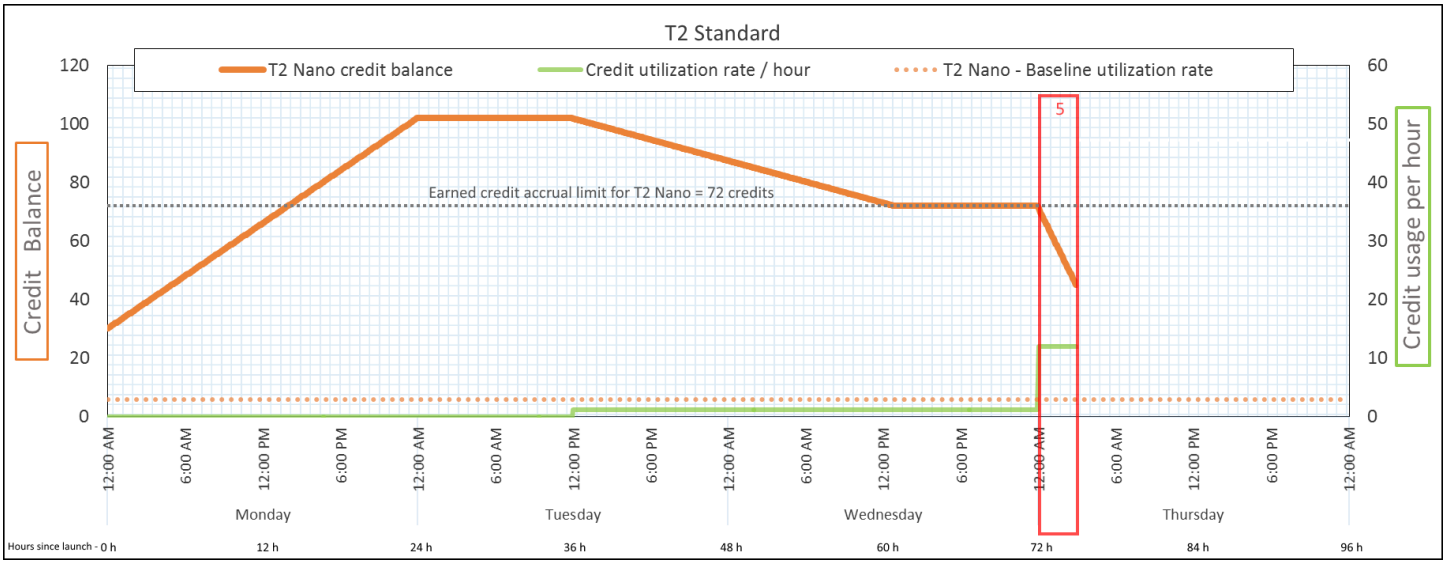
	obtención de créditos): 13,2 créditos— en 11 horas
Tasa de obtención de créditos	72 créditos cada 24 horas
Tasa de descarte de créditos	43.2 créditos cada 24 horas (60% de tasa de obtención de créditos)
Saldo de créditos	72 créditos (0 créditos de inicialización, 72 créditos obtenidos) — el saldo ha alcanzado su límite

Conclusión

Una vez que se han gastado los créditos de inicialización, el límite del saldo de créditos viene determinado por el número de créditos que puede obtener una instancia en 24 horas. Si una instancia obtiene más créditos de los que gasta, se descartarán los créditos obtenidos que superen el límite.

Periodo 5: 73 – 75 horas

Durante las siguientes tres horas, la instancia llega al 20% de uso de la CPU, lo que requiere 36 créditos. La instancia obtiene nueve créditos durante las mismas tres horas, lo que da como resultado una disminución neta del saldo de 27 créditos. Al finalizar las tres horas, el saldo de créditos es de 45 créditos obtenidos acumulados.



Tasa de gasto de créditos	288 créditos cada 24 horas (12 créditos por hora, 20% de uso de la CPU, 400% de tasa de obtención de créditos): 36 créditos— en 3 horas
Tasa de obtención de créditos	72 créditos cada 24 horas (9 créditos en 3 horas)
Tasa de descarte de créditos	0 créditos cada 24 horas
Saldo de créditos	45 créditos (saldo anterior (72) - créditos gastados (36) + créditos obtenidos (9)) — el saldo disminuye a un ritmo de 216 créditos cada 24 horas (tasa de gasto 288/24 + tasa de obtención 72/24 = tasa de disminución del saldo 216/24)

Conclusión

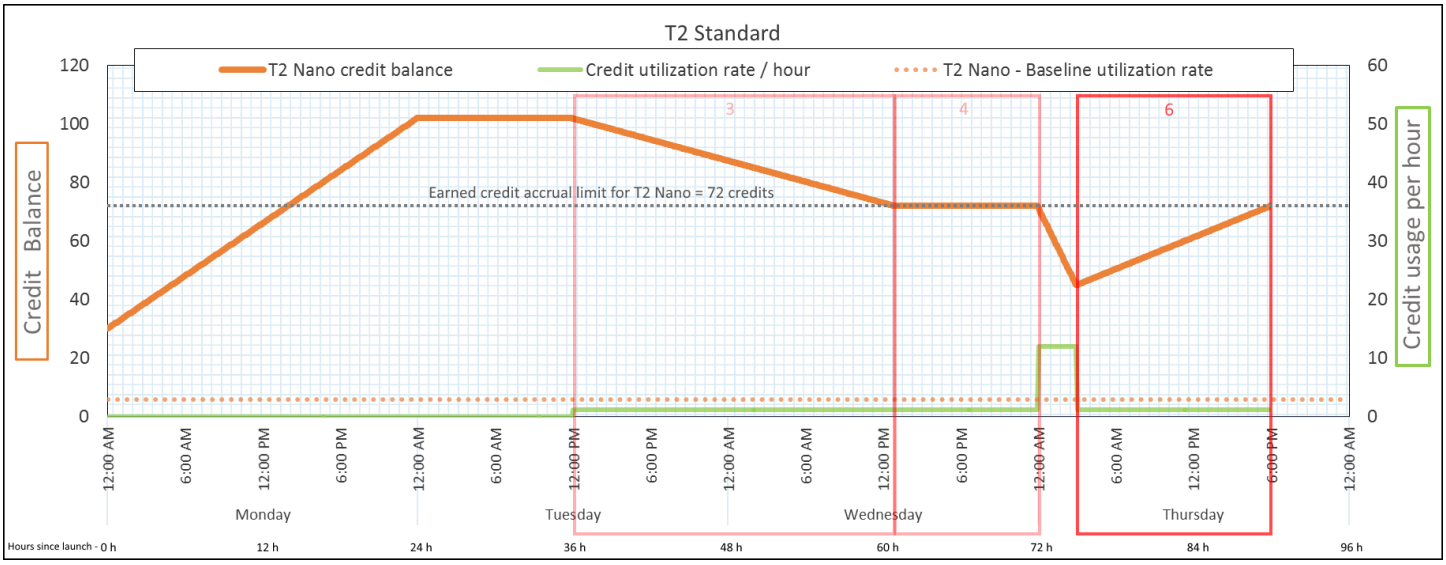
Si una instancia gasta más créditos de los que obtiene, su saldo de créditos disminuye.

Periodo 6: 76 – 90 horas

Durante las siguientes 15 horas, la instancia utiliza el 2% de la CPU, lo que requiere 18 créditos. Este es el mismo uso de la CPU que en los períodos 3 y 4. Sin embargo, el saldo aumenta en este periodo, mientras que disminuyó en el periodo 3 y se estabilizó en el periodo 4.

En el periodo 3, los créditos de inicialización acumulados se gastaron, y los créditos recién obtenidos que superaban el límite de créditos se descartaron, dando como resultado una disminución del saldo de créditos. En el periodo 4, la instancia ha gastado menos créditos de los que ha obtenido. Los créditos obtenidos que superaban el límite se descartaron, por lo que el saldo se mantuvo en su máximo de 72 créditos.

En este periodo no hay créditos de inicialización acumulados, y el número de créditos obtenidos acumulados en el saldo está por debajo del límite. No se ha descartado ningún crédito obtenido. Además, la instancia obtiene más créditos de los que gasta, lo que da como resultado un incremento en el saldo de créditos.



Tasa de gasto de créditos	28,8 créditos cada 24 horas (1,2 créditos por hora, 2% de uso de la CPU, 40% de tasa de obtención de créditos): 18 créditos— en 15 horas
Tasa de obtención de créditos	72 créditos cada 24 horas (45 créditos en 15 horas)
Tasa de descarte de créditos	0 créditos cada 24 horas
Saldo de créditos	72 créditos (el saldo aumenta a un ritmo de 43,2 créditos— cada 24 horas: tasa de cambio = tasa de gasto 28,8/24 + tasa de obtención 72/24)

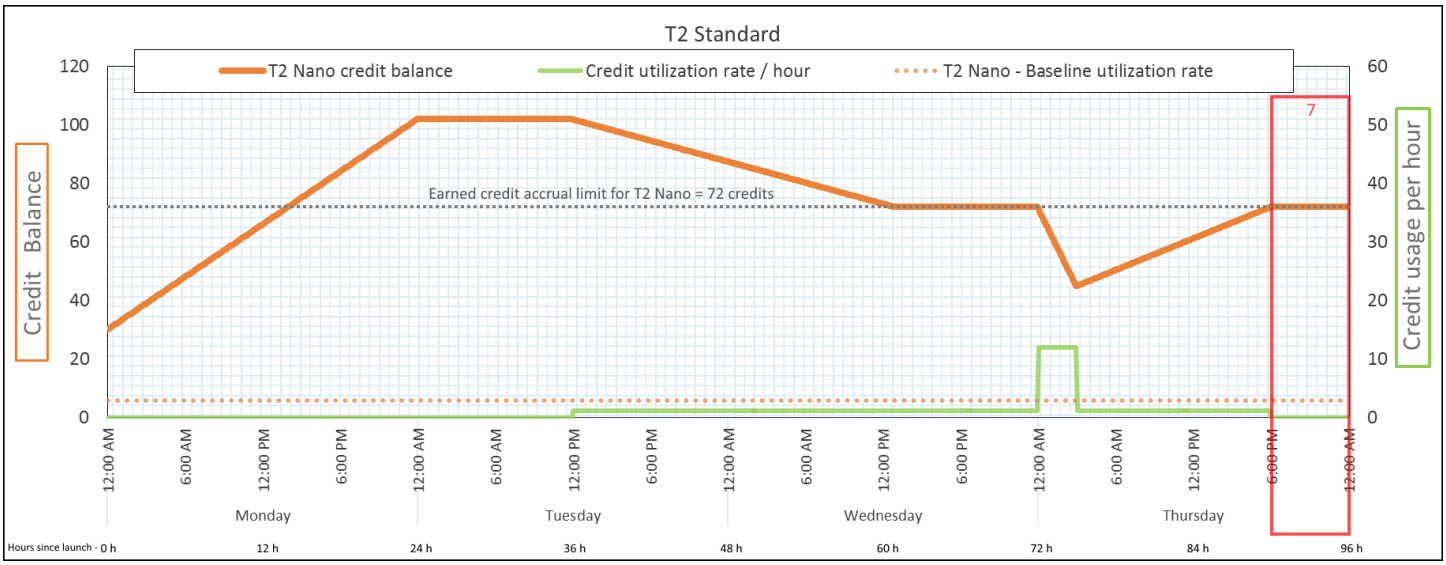
Conclusión

Si una instancia gasta menos créditos de los que obtiene, su saldo de créditos aumenta.

Periodo 7: 91 – 96 horas

Durante las seis horas siguientes, la instancia —permanece inactiva —(el uso de la CPU es del 0 %) y no se gasta ningún crédito. Este es el mismo uso de la CPU que el del periodo 2, pero el saldo no se detiene en 102 créditos, se detiene —en 72 créditos, que es el límite de saldo de créditos de la instancia.

En el periodo 2, el saldo de créditos incluía 30 créditos de inicialización acumulados. Los créditos de inicialización se gastaron en el periodo 3. Una instancia en ejecución no puede obtener más créditos de inicialización. Una vez alcanzado el límite de saldo de créditos, se descartarán todos los créditos obtenidos que superen dicho límite.



Tasa de gasto de créditos	0 créditos cada 24 horas (0% de uso de la CPU)
Tasa de obtención de créditos	72 créditos cada 24 horas
Tasa de descarte de créditos	72 créditos cada 24 horas (100% de tasa de obtención de créditos)
Saldo de créditos	72 créditos (0 créditos de inicialización, 72 créditos obtenidos)

Conclusión

Una instancia obtiene créditos constantemente, pero no puede acumular más créditos obtenidos si se ha alcanzado el límite de saldo de créditos. Una vez que se ha alcanzado el límite, cualquier nuevo crédito que se obtenga se descarta. El límite de saldo de créditos viene determinado por el número de créditos que puede obtener una instancia en 24 horas. Para obtener más información acerca de los límites de saldo de créditos, consulte la tabla de créditos.

Trabajo con instancias de rendimiento ampliables

Los pasos para iniciar, supervisar y modificar estas instancias de rendimiento ampliable (instancias T) son similares. La diferencia principal es la especificación de crédito predeterminada en la inicialización.

Cada familia de instancias T incluye la siguiente especificación de crédito predeterminada:

- Las instancias T4g, T3a y T3 se inician como `unlimited`
- Las instancias T3 en un host dedicado se inician como `standard`
- Las instancias T2 se inician como `standard`

Puede cambiar la especificación de crédito predeterminada para la cuenta.

Contenido

Para iniciar una instancia de rendimiento ampliable como ilimitada o estándar

Puede iniciar sus instancias T como `unlimited` o `standard` mediante la consola de Amazon EC2, un AWS SDK, una herramienta de línea de comandos o un grupo de escalado automático.

En los siguientes procedimientos, se describe cómo usar la consola de EC2 o la AWS CLI. Para obtener información sobre el uso de un grupo de escalado automático, consulte Uso de un grupo de Auto Scaling para iniciar una instancia de rendimiento ampliable como ilimitada.

Console

inicialización de una instancia T como Unlimited o Standard

1. Siga el procedimiento para lanzar una instancia.

2. En Instance type (Tipo de instancia), elija un tipo de instancia T.
3. Expanda Advanced details (Detalles avanzados) y, en Credit specification (Especificación de crédito), seleccione una especificación de crédito. Si no selecciona ninguna opción, se utilizará el valor predeterminado, que es `standard` para T2, y `unlimited` para T4g, T3a y T3.
4. En el panel Summary (Resumen), revise la configuración de la instancia y, a continuación, elija Launch instance (iniciar instancia). Para obtener más información, consulte Lance una instancia con el nuevo asistente de inicialización de instancias.

AWS CLI

inicialización de una instancia T como Unlimited o Standard

Utilice el comando run-instances para iniciar sus instancias. Elija la especificación de crédito mediante el parámetro `--credit-specification CpuCredits=`. Las especificaciones de crédito válidas son `unlimited` y `standard`.

- Para el caso de T4g, T3a y T3, si no incluye el parámetro `--credit-specification`, la instancia se inicia como `unlimited` de forma predeterminada.
- En el caso de T2, si no incluye el parámetro `--credit-specification`, la instancia se inicia como `standard` de forma predeterminada.

```
aws ec2 run-instances \
    --image-id ami-abc12345 \
    --count 1 \
    --instance-type t3.micro \
    --key-name MyKeyPair \
    --credit-specification "CpuCredits=unlimited"
```

Uso de un grupo de Auto Scaling para iniciar una instancia de rendimiento ampliable como ilimitada

Cuando las instancias T se inician o inician, necesitan créditos de CPU para obtener una buena experiencia durante el proceso de arranque. Si utiliza un grupo de Auto Scaling para iniciar las instancias, recomendamos que configure las instancias como `unlimited`. Si lo hace, las instancias utilizan créditos sobrantes cuando el grupo de Auto Scaling las inicia o las reinicia automáticamente. Usar créditos sobrantes evita que haya posibles restricciones de rendimiento.

Crear una plantilla de lanzamiento

Debe utilizar una plantilla de inicialización para iniciar instancias como `unlimited` en un grupo de Auto Scaling. La configuración de inicialización no permite iniciar instancias como `unlimited`.

> **Note**
>
> El modo `unlimited` no es compatible con las instancias T3 que se inician en un host dedicado.

Console

Para crear una plantilla de inicialización que lance instancias como Unlimited

1. Siga el procedimiento Crear una plantilla de lanzamiento mediante la configuración avanzada en la Guía del usuario de Amazon EC2 Auto Scaling.
2. En Launch template contents (Contenido de la plantilla de inicialización), para Instance type (Tipo de instancia), elija un tamaño de instancia.
3. Para iniciar instancias como `unlimited` en un grupo de Auto Scaling, en Advanced details (Detalles avanzados), para Credit specification (Especificación de crédito), elija Unlimited (Ilimitado).
4. Cuando haya terminado de definir los parámetros de la plantilla de inicialización, elija Create launch template (Crear plantilla de inicialización).

AWS CLI

Para crear una plantilla de inicialización que lance instancias como Unlimited

Utilice el comando create-launch-template y especifique `unlimited` como especificación de crédito.

- Para el caso de T4g, T3a y T3, si no incluye el valor `CreditSpecification={CpuCredits=unlimited}`, la instancia se inicia como `unlimited` de forma predeterminada.
- En el caso de T2, si no incluye el valor `CreditSpecification={CpuCredits=unlimited}`, la instancia se inicia como `standard` de forma predeterminada.

```
aws ec2 create-launch-template \
    --launch-template-name MyLaunchTemplate \
    --version-description FirstVersion \
    --launch-template-data
 ImageId=ami-8c1be5f6,InstanceType=t3.medium,CreditSpecification={CpuCredits=unlimited}
```

Asociación de un grupo de Auto Scaling con una plantilla de inicialización

Para asociar la plantilla de inicialización a un grupo de Auto Scaling, cree el grupo de Auto Scaling con la plantilla de inicialización o añada dicha plantilla a un grupo de Auto Scaling existente.

Console

Crear un grupo de escalado automático mediante una plantilla de inicialización

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la barra de navegación de la parte superior de la pantalla, seleccione la misma región que utilizó cuando creó la plantilla de inicialización.
3. En el panel de navegación, elija Auto Scaling Groups (Grupos de), Create Auto Scaling group (Crear grupo de).
4. Elija Launch Template (Plantilla de inicialización), seleccione la plantilla de inicialización y, a continuación, elija Next Step (Paso siguiente).
5. Complete los campos para el grupo de Auto Scaling. Cuando haya terminado de revisar las opciones de configuración de la página Review (Revisar), elija Create Auto Scaling group (Crear grupo de Auto Scaling). Para obtener más información, consulte Crear un grupo de escalado automático mediante una plantilla de inicialización en la Guía del usuario de Amazon EC2 Auto Scaling.

AWS CLI

Crear un grupo de escalado automático mediante una plantilla de inicialización

Ejecute el comando create-auto-scaling-group de la AWS CLI y especifique el parámetro `--launch-template`.

Console

Agregar una plantilla de inicialización a un grupo de escalado automático existente

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la barra de navegación de la parte superior de la pantalla, seleccione la misma región que utilizó cuando creó la plantilla de inicialización.
3. En el panel de navegación, elija Auto Scaling Groups (Grupos de).
4. En la lista de grupos de Auto Scaling, seleccione un grupo de Auto Scaling y elija Actions (Acciones), Edit (Editar).
5. En la pestaña Details (Detalles), en Launch Template (Plantilla de inicialización), elija una plantilla de inicialización y, a continuación, Save (Guardar).

AWS CLI

Agregar una plantilla de inicialización a un grupo de escalado automático existente

Ejecute el comando update-auto-scaling-group de la AWS CLI y especifique el parámetro `--launch-template`.

Ver la especificación de crédito de una instancia de rendimiento ampliable

Puede ver la especificación de crédito (`unlimited` o `standard`) de una instancia T en ejecución o detenida.

Console

Visualización de la especificación de crédito de una instancia T

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación izquierdo, elija Instances.
3. Seleccione la instancia.
4. Elija Details (Detalles) y consulte la información del campo Credit specification (Especificación de crédito). El valor es `unlimited` o `standard`.

AWS CLI

Descripción de la especificación de crédito de una instancia T

Utilice el comando describe-instance-credit-specifications. Si no especifica uno o varios identificadores de instancia, se devuelven todas las instancias con la opción de crédito `unlimited`, así como las instancias que se configuraron previamente con la especificación de crédito `unlimited`. Por ejemplo, si redimensiona una instancia T3 a una instancia M4, mientras está configurada como `unlimited`, Amazon EC2 devuelve la instancia M4.

```
aws ec2 describe-instance-credit-specifications --instance-id i-1234567890abcdef0
```

Ejemplo de resultado

```
{
  "InstanceCreditSpecifications": [
    {
        "InstanceId": "i-1234567890abcdef0",
        "CpuCredits": "unlimited"
    }
  ]
}
```

Modificación de la especificación de crédito de una instancia de rendimiento ampliable

Puede cambiar la especificación de crédito de una instancia T en ejecución o detenida en cualquier momento entre `unlimited` y `standard`.

Tenga en cuenta que, en el modo `unlimited`, una instancia puede gastar los créditos sobrantes, lo que podría generar un cargo adicional. Para obtener más información, consulte Los créditos sobrantes pueden generar costos.

Console

Modificación de la especificación de crédito de una instancia T

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación izquierdo, elija Instances.
3. Seleccione la instancia. Para modificar la especificación de crédito de varias instancias a la vez, seleccione todas las instancias aplicables.
4. Elija Actions (Acciones), Instance settings (Configuración de la instancia), Change credit specification (Cambiar especificación de crédito). Esta opción solo se activa si ha seleccionado una instancia T.

5. Para cambiar la especificación de crédito a `unlimited`, active la casilla de verificación situada junto al ID de instancia. Para cambiar la especificación de crédito a `standard`, desactive la casilla de verificación situada junto al ID de instancia.

AWS CLI

Modificación de la especificación de crédito de una instancia T

Utilice el comando modify-instance-credit-specification. Especifique la instancia y su especificación de crédito mediante el parámetro `--instance-credit-specification`. Las especificaciones de crédito válidas son `unlimited` y `standard`.

```
aws ec2 modify-instance-credit-specification \
    --region us-east-1 \
    --instance-credit-specification
 "InstanceId=i-1234567890abcdef0,CpuCredits=unlimited"
```

Ejemplo de resultado

```
{
  "SuccessfulInstanceCreditSpecifications": [
    {
      "InstanceId": "i- 1234567890abcdef0"
    }
  ],
  "UnsuccessfulInstanceCreditSpecifications": []
}
```

Configuración de la especificación de crédito predeterminada para la cuenta

Cada familia de instancias T incluye una especificación de crédito predeterminada. Puede cambiar la especificación de crédito predeterminada de cada familia de instancias T en las cuentas por región de AWS.

Si utiliza el asistente de inicialización de instancias en la consola de EC2 para iniciar instancias, el valor que seleccione para la especificación de crédito invalida la especificación de crédito predeterminada de las cuentas. Si utiliza AWS CLI para iniciar instancias, todas las instancias T nuevas de la cuenta se inician mediante la especificación de crédito predeterminada. La especificación de crédito para las instancias existentes en ejecución o detenidas no se ve afectada.

Consideración

La especificación de crédito predeterminada de una familia de instancias solo se puede modificar una vez en un periodo de 5 minutos y hasta cuatro veces en un periodo de 24 horas sucesivas.

Console

Para establecer la especificación de crédito predeterminada de las cuentas por región

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. En el panel de navegación izquierdo, elija Panel de EC2.
4. En Account attributes (Atributos de cuenta), seleccione Default credit specification (Especificación de crédito predeterminada).
5. Seleccione Manage (Administrar).
6. Para cada familia de instancias, elija Unlimited (Ilimitado) o Standard (Estándar)y, a continuación, seleccione Update (Actualizar).

AWS CLI

Para establecer la especificación de crédito predeterminada en el nivel de cuenta (AWS CLI)

Utilice el comando modify-default-credit-specification. Especifique la región de AWS, la familia de instancias y la especificación de crédito predeterminada mediante el parámetro `--cpu-credits`. Las especificaciones de crédito predeterminadas válidas son `unlimited` y `standard`.

```
aws ec2 modify-default-credit-specification \
    --region us-east-1 \
    --instance-family t2 \
    --cpu-credits unlimited
```

Consulta de la especificación de crédito predeterminada

Puede ver la especificación de crédito predeterminada de una familia de instancias T en la cuenta por región de AWS.

Console

Visualización de la especificación de crédito predeterminada en la cuenta

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. En el panel de navegación izquierdo, elija Panel de EC2.
4. En Account attributes (Atributos de cuenta), seleccione Default credit specification (Especificación de crédito predeterminada).

AWS CLI

Visualización de la especificación de crédito predeterminada en la cuenta

Utilice el comando get-default-credit-specification. Especifique la región y la familia de instancias de AWS.

```
aws ec2 get-default-credit-specification --region us-east-1 --instance-family t2
```

Supervisión de los créditos de su CPU en busca de instancias de rendimiento ampliable

Amazon EC2 envía métricas a Amazon CloudWatch. Puede ver las métricas de crédito de CPU en las métricas por instancia de Amazon EC2 de la consola de CloudWatch o mediante la AWS CLI para enumerar las métricas de cada instancia. Para obtener más información, consulte Enumerar las métricas con la consola y Enumerar las métricas con la AWS CLI.

Contenido

Métricas de CloudWatch adicionales para las instancias de rendimiento ampliable

Las instancias de rendimiento ampliable tienen estas métricas de CloudWatch adicionales, que se actualizan cada cinco minutos:

- `CPUCreditUsage` – el número total de créditos de CPU que se han gastado durante el periodo de medición.
- `CPUCreditBalance` – el número de créditos de la CPU que ha acumulado una instancia. Este saldo se agota cuando la CPU realiza ráfagas y los créditos de CPU se gastan más rápido de lo que se obtienen.
- `CPUSurplusCreditBalance` – el número de créditos de CPU sobrantes que se han gastado para mantener la utilización de la CPU cuando el valor de `CPUCreditBalance` es igual a cero.
- `CPUSurplusCreditsCharged` – el número de créditos de CPU sobrantes que superen la cantidad máxima de créditos de CPU que se pueden obtener en un periodo de 24 horas y que, por lo tanto, generan gastos adicionales.

Las dos últimas métricas son aplicables solo a instancias configuradas como `unlimited`.

En la siguiente tabla se describen las métricas de CloudWatch para instancias de rendimiento ampliable. Para obtener más información, consulte Mostrar las métricas de CloudWatch disponibles para las instancias.

Métrica	Descripción
`CPUCreditUsage`	La cantidad de créditos de CPU gastados por la instancia para la utilización de la CPU. Un crédito de CPU equivale a una vCPU ejecutándose al 100% de utilización durante un minuto o una combinación equivalente de unidades de vCPU, utilización y tiempo (por ejemplo, una vCPU ejecutándose al 50% durante dos minutos o dos vCPU ejecutándose al 25% durante dos minutos). Las métricas de créditos de CPU solo están disponibles cada cinco minutos. Si especifica un periodo superior a cinco minutos, use la estadística `Sum` en lugar de `Average`. Unidades: créditos (vCPU/minutos)
`CPUCreditBalance`	La cantidad de créditos de la CPU obtenidos que una instancia ha acumulado desde que se lanzó o se inició. Para T2 Standard, el `CPUCreditBalance` incluye además el número de créditos de inicialización que se han acumulado.

Métrica	Descripción
	Los créditos se acumulan en el saldo de créditos una vez obtenidos y se eliminan del saldo de créditos cuando se gastan. El saldo de créditos tiene un límite máximo, determinado por el tamaño de la instancia. Una vez que se ha alcanzado el límite, los nuevos créditos obtenidos se descartarán. Para T2 Standard, los créditos de inicialización no cuentan para el límite. Los créditos de `CPUCreditBalance` están disponibles para que la instancia los gaste a fin de aumentar la utilización de la CPU por encima de la referencia. Cuando una instancia está en ejecución, los créditos en el `CPUCreditBalance` no caducan. Cuando se detiene una instancia T4g, T3a o T3, el valor `CPUCreditBalance` se mantiene durante siete días. A partir de ese momento, se pierden todos los créditos acumulados. Cuando se detiene una instancia T2, el valor de `CPUCreditBalance` no se mantiene y se pierden todos los créditos acumulados. Las métricas de créditos de CPU solo están disponibles cada cinco minutos. Unidades: créditos (vCPU/minutos)
`CPUSurplusCreditBalance`	La cantidad de créditos sobrantes que ha gastado una instancia `unlimited` cuando su valor `CPUCreditBalance` es igual a cero. El valor de `CPUSurplusCreditBalance` se compensa con los créditos de CPU obtenidos. Si el número de créditos sobrantes supera el número máximo de créditos que la instancia puede ganar en un periodo de 24 horas, los créditos sobrantes gastados por encima del máximo implican un cargo adicional. Unidades: créditos (vCPU/minutos)

Métrica	Descripción
`CPUSurplusCreditsCharged`	La cantidad de créditos sobrantes gastados que no se han compensado con créditos de CPU obtenido y, por lo tanto, implican un cargo adicional. Los créditos sobrantes gastados se cobran cuando se da alguno de los casos siguientes: • Los créditos sobrantes gastados superan el número máximo de créditos que la instancia puede obtener en un periodo de 24 horas. Los créditos sobrantes gastados por encima de la cantidad máxima se cobran al final de la hora. • La instancia se detiene o se termina. • La instancia se cambia de `unlimited` a `standard`. Unidades: créditos (vCPU/minutos)

Calcular el uso de crédito de CPU

El uso de créditos de CPU en las instancias se calcula mediante las métricas de CloudWatch de las instancias descritas en la tabla anterior.

Amazon EC2 envía las métricas a CloudWatch cada cinco minutos. Una referencia al valor anterior de una métrica en cualquier momento implica el valor previo de la métrica enviado hace 5 minutos.

Calcular el uso del crédito de la CPU para instancias estándar

- El saldo de créditos de CPU aumenta si el uso de la CPU cae por debajo de la base de referencia, cuando la cantidad de créditos gastados es menor que la obtenida en el intervalo anterior de 5 minutos.
- El saldo de créditos de CPU disminuye si el uso de la CPU supera la base de referencia, cuando la cantidad de créditos gastados es mayor que la obtenida en el intervalo anterior de 5 minutos.

La siguiente ecuación representa esta operación matemáticamente:

Example

```
CPUCreditBalance = prior CPUCreditBalance + [Credits earned per hour * (5/60) -
 CPUCreditUsage]
```

El tamaño de la instancia determina el número de créditos que la instancia puede obtener por hora y el número de créditos obtenidos que puede acumular en el saldo de crédito. Para obtener más información acerca de la cantidad de créditos obtenidos por hora y del límite de saldo de crédito en función del tamaño de la instancia, consulte la tabla de crédito.

Ejemplo

En este ejemplo se utiliza una instancia `t3.nano`. Para calcular el valor de `CPUCreditBalance` de la instancia, utilice la ecuación anterior como se indica a continuación:

- `CPUCreditBalance` – el saldo de créditos actual que desea calcular.
- `prior CPUCreditBalance` – el saldo de créditos de hace cinco minutos. En este ejemplo, la instancia ha acumulado 2 créditos.
- `Credits earned per hour` – una instancia `t3.nano` obtiene seis créditos por hora.
- `5/60`: representa – el intervalo de cinco minutos entre la publicación de métricas de CloudWatch. Multiplique los créditos obtenidos por hora por 5/60 (cinco minutos) para obtener la cantidad de créditos que la instancia ha adquirido en los últimos cinco minutos. Una instancia `t3.nano` obtiene 0,5 créditos cada 5 minutos.
- `CPUCreditUsage`: la cantidad – de créditos que ha gastado la instancia en los últimos cinco minutos. En este ejemplo, la instancia ha gastado 1 crédito en los últimos 5 minutos.

Utilizando estos valores, puede calcular el de `CPUCreditBalance`:

Example

```
CPUCreditBalance = 2 + [0.5 - 1] = 1.5
```

Calcular el uso del crédito de la CPU para instancias ilimitadas

Cuando una instancia de rendimiento ampliable necesita aumentar su uso por encima del nivel de referencia, siempre gasta sus créditos acumulados antes de gastar los créditos sobrantes. Una vez que agota su saldo de créditos de CPU acumulados, puede gastar créditos sobrantes para realizar ráfagas en la CPU durante tanto tiempo como sea necesario. Cuando la utilización de la CPU de

una instancia cae por debajo de la base de referencia, los créditos sobrantes siempre se compensan antes de que la instancia acumule créditos obtenidos.

Utilizamos el término `Adjusted balance` en las siguientes ecuaciones para reflejar la actividad que ocurre en este intervalo de 5 minutos. Utilizamos este valor para llegar a los valores de las métricas `CPUCreditBalance` y `CPUSurplusCreditBalance` de CloudWatch.

Example

```
Adjusted balance = [prior CPUCreditBalance - prior CPUSurplusCreditBalance] + [Credits
 earned per hour * (5/60) - CPUCreditUsage]
```

El valor `0` en `Adjusted balance` indica que la instancia ha gastado todos los créditos obtenidos para transmisión por ráfaga y que no se gastaron créditos sobrantes. Como resultado de ello, los valores de `CPUCreditBalance` y `CPUSurplusCreditBalance` son `0`.

Un valor `Adjusted balance` positivo indica que la instancia ha acumulado los créditos obtenidos y que los créditos sobrantes, de haberlos, se compensaron. Como resultado de ello, se le asigna el valor `Adjusted balance` a `CPUCreditBalance` y el valor de `CPUSurplusCreditBalance` pasa a `0`. El tamaño de la instancia determina el número de créditos máximo que puede acumular.

Example

```
CPUCreditBalance = min [max earned credit balance, Adjusted balance]
CPUSurplusCreditBalance = 0
```

Un valor `Adjusted balance` negativo indica que la instancia ha gastado todos los créditos obtenidos que ha acumulado y los créditos sobrantes para realizar ráfagas. Como resultado de ello, se le asigna el valor `Adjusted balance` a `CPUSurplusCreditBalance` y `CPUCreditBalance` se establece en `0`. Nuevamente, el tamaño de la instancia determina el número de créditos máximo que puede acumular.

Example

```
CPUSurplusCreditBalance = min [max earned credit balance, -Adjusted balance]
CPUCreditBalance = 0
```

Si los créditos sobrantes gastados superan la cantidad máxima de créditos que puede acumular la instancia, el saldo de créditos sobrantes se establece en el máximo, tal como se muestra en la

ecuación anterior. Los créditos sobrantes que queden, se cobran tal como se representan en a métrica `CPUSurplusCreditsCharged`.

Example

```
CPUSurplusCreditsCharged = max [-Adjusted balance - max earned credit balance, 0]
```

Finalmente, cuando se termina la instancia, se cobran los créditos sobrantes correspondientes al valor de `CPUSurplusCreditBalance`. Si la instancia cambia de `unlimited` a `standard`, el saldo `CPUSurplusCreditBalance` restante también se cobra.

Aceleración del rendimiento con instancias de GPU

Las instancias basadas en GPU ofrecen acceso a GPU de NVIDIA con miles de núcleos de computación. Puede utilizar estas instancias para acelerar aplicaciones científicas, de ingeniería y de renderizado aprovechando los marcos de trabajo de computación paralela CUDA u Open Computing Language (OpenCL). También las puede utilizar para aplicaciones de gráficos, incluido el streaming de juegos, el streaming de aplicaciones 3-D y otras cargas de trabajo de gráficos.

Antes de activar u optimizar una instancia basada en GPU, debe instalar los controladores adecuados de la siguiente manera:

- Para instalar controladores NVIDIA en una instancia con una GPU NVIDIA conectada, como una instancia P3 o G4dn, consulte Instalación de controladores NVIDIA.
- Para instalar controladores AMD en una instancia con una GPU AMD asociada, como una instancia G4ad, consulte Instalar controladores AMD.

Contenido

Activación de las aplicaciones virtuales NVIDIA GRID en las instancias de Amazon EC2 basadas en GPU

Para activar las aplicaciones virtuales de GRID en instancias basadas en GPU que tienen GPU NVIDIA (el escritorio virtual de NVIDIA GRID está habilitado de forma predeterminada), debe definir el tipo de producto para el controlador de la siguiente manera.

Activación de las aplicaciones virtuales de GRID en instancias de Linux

1. Cree el archivo `/etc/nvidia/gridd.conf` a partir del archivo de plantilla proporcionado.

   ```
   [ec2-user ~]$ sudo cp /etc/nvidia/gridd.conf.template /etc/nvidia/gridd.conf
   ```

2. Abra el archivo `/etc/nvidia/gridd.conf` en el editor de texto que prefiera.
3. Encuentre la línea `FeatureType` y configúrela igual a `0`. A continuación, añada una línea con `IgnoreSP=TRUE`.

   ```
   FeatureType=0 IgnoreSP=TRUE
   ```

4. Guarde el archivo y salga de él.
5. Reinicie la instancia para actualizar la nueva configuración.

   ```
   [ec2-user ~]$ sudo reboot
   ```

Activación de las aplicaciones virtuales de GRID en instancias de Windows

Activación de las aplicaciones virtuales de GRID en instancias de Windows

1. Ejecute regedit.exe para abrir el Editor del Registro.
2. Vaya a `HKEY_LOCAL_MACHINE\SOFTWARE\NVIDIA Corporation\Global\GridLicensing`.
3. Abra el menú contextual (haga clic con el botón derecho) en el panel derecho y elija Nuevo, Valor de DWORD.
4. En Name (Nombre), escriba FeatureType y pulse `Enter`.
5. Abra el menú contextual (haga clic con el botón derecho) de FeatureType y elija Modificar.
6. En Información del valor, introduzca `0` para aplicaciones virtuales de NVIDIA GRID y elija Aceptar.

7. Abra el menú contextual (haga clic con el botón derecho) en el panel derecho y elija Nuevo, Valor de DWORD.
8. Para Name, escriba IgnoreSP y pulse `Enter`.
9. Abra vez el menú contextual (haga clic con el botón derecho) de IgnoreSP y elija Modificar.
10. En Información del valor, escriba 1 y elija Aceptar.
11. Cierre el editor de registro.

Optimización de las configuraciones de GPU en instancias de Amazon EC2

Existen varias optimizaciones de configuración de GPU que puede llevar a cabo para lograr el mejor rendimiento en sus instancias de NVIDIA GPU. Con algunos de estos tipos de instancias, el controlador NVIDIA utiliza una función de mejora automática, que varía las velocidades del reloj de la GPU. Al deshabilitar la característica de mejora de potencia automática y al ajustar las velocidades de reloj de GPU a la frecuencia máxima, puede obtener de forma uniforme el rendimiento máximo de las instancias de GPU.

Optimización de las configuraciones de GPU en Linux

1. Configure los ajustes de GPU para que sean persistentes. Este comando puede tardar varios minutos en ejecutarse.

   ```
   [ec2-user ~]$ sudo nvidia-persistenced
   ```

2. [Solo para instancias G3 y P2] Desactive la característica de mejora de potencia automática para todas las GPU de la instancia.

   ```
   [ec2-user ~]$ sudo nvidia-smi --auto-boost-default=0
   ```

3. Ajuste todas las velocidades de reloj de GPU a la frecuencia máxima. Utilice las velocidades de reloj de gráficos y memoria especificadas en los siguientes comandos.

   Algunas versiones del controlador NVIDIA no admiten la configuración de la velocidad del reloj de la aplicación y muestran el error "`Setting applications clocks is not supported for GPU...`", que puede ignorar.

   - instancias G3:

     ```
     [ec2-user ~]$ sudo nvidia-smi -ac 2505,1177
     ```

- instancias G4dn:

```
[ec2-user ~]$ sudo nvidia-smi -ac 5001,1590
```

- instancias G5:

```
[ec2-user ~]$ sudo nvidia-smi -ac 6250,1710
```

- Instancias G6 y Gr6:

```
[ec2-user ~]$ sudo nvidia-smi -ac 6251,2040
```

- instancias P2:

```
[ec2-user ~]$ sudo nvidia-smi -ac 2505,875
```

- instancias P3 y P3dn:

```
[ec2-user ~]$ sudo nvidia-smi -ac 877,1530
```

- instancias P4d:

```
[ec2-user ~]$ sudo nvidia-smi -ac 1215,1410
```

- instancias P4de:

```
[ec2-user ~]$ sudo nvidia-smi -ac 1593,1410
```

- instancias P5:

```
[ec2-user ~]$ sudo nvidia-smi -ac 2619,1980
```

Optimización de las configuraciones de GPU en Windows

1. Abra una ventana de PowerShell y desplácese hasta la carpeta de instalación de NVIDIA.

```
cd "C:\Windows\System32\DriverStore\FileRepository\nv_dispswi.inf_*\"
```

2. [Solo para instancias G3 y P2] Desactive la característica de mejora de potencia automática para todas las GPU de la instancia.

```
.\nvidia-smi --auto-boost-default=0
```

3. Ajuste todas las velocidades de reloj de GPU a la frecuencia máxima. Utilice las velocidades de reloj de gráficos y memoria especificadas en los siguientes comandos.

   Algunas versiones del controlador NVIDIA no admiten la configuración de la velocidad del reloj de la aplicación y muestran el error "`Setting applications clocks is not supported for GPU...`", que puede ignorar.

   - instancias G3:

     ```
     .\nvidia-smi -ac "2505,1177"
     ```

   - instancias G4dn:

     ```
     .\nvidia-smi -ac "5001,1590"
     ```

   - instancias G5:

     ```
     .\nvidia-smi -ac "6250,1710"
     ```

   - Instancias G6 y Gr6:

     ```
     .\nvidia-smi -ac "6251,2040"
     ```

   - instancias P2:

     ```
     .\nvidia-smi -ac "2505,875"
     ```

   - instancias P3 y P3dn:

     ```
     .\nvidia-smi -ac "877,1530"
     ```

   - instancias P4d:

     ```
     [ec2-user ~]$ sudo nvidia-smi -ac 1215,1410
     ```

   - instancias P4de:

     ```
     [ec2-user ~]$ sudo nvidia-smi -ac 1593,1410
     ```

- instancias P5:

```
[ec2-user ~]$ sudo nvidia-smi -ac 2619,1980
```

Configuración de pantallas 4K duales en instancias de Linux G4ad

inicialización de una instancia G4ad

1. Conéctese a su instancia Linux para obtener la dirección de bus PCI de la GPU a la que desea orientar para 4K dual (2x4k):

   ```
   lspci -vv | grep -i amd
   ```

   Obtendrá un resultado similar al siguiente:

   ```
   00:1e.0 Display controller: Advanced Micro Devices, Inc. [*AMD*/ATI] Device 7362 (rev
    c3)
   Subsystem: Advanced Micro Devices, Inc. [AMD/ATI] Device 0a34
   ```

2. Note que la dirección de bus PCI es 00:1e.0 en la salida anterior. Cree un archivo denominado `/etc/modprobe.d/amdgpu.conf` y agregue:

   ```
   options amdgpu virtual_display=0000:00:1e.0,2
   ```

3. Para instalar los controladores AMD en Linux, consulte Instalación de controladores AMD en su instancia de Amazon EC2. Si ya tiene instalado el controlador de GPU AMD, tendrá que reconstruir los módulos del kernel amdgpu a través de dkms.

4. Use el siguiente archivo xorg.conf para definir la topología de pantalla dual (2x4K) y guarde el archivo en `/etc/X11/xorg.conf:`

   ```
   ~$ cat /etc/X11/xorg.conf
   Section "ServerLayout"
       Identifier     "Layout0"
       Screen          0 "Screen0"
       Screen        1 "Screen1"
       InputDevice     "Keyboard0" "CoreKeyboard"
       InputDevice     "Mouse0" "CorePointer"
       Option          "Xinerama" "1"
   EndSection
   ```

```
Section "Files"
    ModulePath "/opt/amdgpu/lib64/xorg/modules/drivers"
    ModulePath "/opt/amdgpu/lib/xorg/modules"
    ModulePath "/opt/amdgpu-pro/lib/xorg/modules/extensions"
    ModulePath "/opt/amdgpu-pro/lib64/xorg/modules/extensions"
    ModulePath "/usr/lib64/xorg/modules"
    ModulePath "/usr/lib/xorg/modules"
EndSection
Section "InputDevice"
    # generated from default
    Identifier     "Mouse0"
    Driver         "mouse"
    Option         "Protocol" "auto"
    Option         "Device" "/dev/psaux"
    Option         "Emulate3Buttons" "no"
    Option         "ZAxisMapping" "4 5"
EndSection
Section "InputDevice"
    # generated from default
    Identifier     "Keyboard0"
    Driver         "kbd"
EndSection

Section "Monitor"
    Identifier     "Virtual"
    VendorName     "Unknown"
    ModelName      "Unknown"
    Option         "Primary" "true"
EndSection

Section "Monitor"
    Identifier     "Virtual-1"
    VendorName     "Unknown"
    ModelName      "Unknown"
    Option         "RightOf" "Virtual"
EndSection

Section "Device"
    Identifier     "Device0"
    Driver         "amdgpu"
    VendorName     "AMD"
    BoardName      "Radeon MxGPU V520"
    BusID          "PCI:0:30:0"
EndSection
```

```
Section "Device"
    Identifier     "Device1"
    Driver         "amdgpu"
    VendorName     "AMD"
    BoardName      "Radeon MxGPU V520"
    BusID          "PCI:0:30:0"
EndSection

Section "Extensions"
    Option         "DPMS" "Disable"
EndSection

Section "Screen"
    Identifier     "Screen0"
    Device         "Device0"
    Monitor        "Virtual"
    DefaultDepth   24
    Option         "AllowEmptyInitialConfiguration" "True"
    SubSection "Display"
        Virtual    3840 2160
        Depth      32
    EndSubSection
EndSection

Section "Screen"
    Identifier     "Screen1"
    Device         "Device1"
    Monitor        "Virtual"
    DefaultDepth   24
    Option         "AllowEmptyInitialConfiguration" "True"
    SubSection "Display"
        Virtual    3840 2160
        Depth      32
    EndSubSection
EndSection
```

5. Configure el DCV con las instrucciones de configuración de unescritorio interactivo.
6. Una vez finalizada la configuración del DCV, reinícielo.
7. Confirme que el controlador esté funcionando:

```
dmesg | grep amdgpu
```

La respuesta debe ser similar a la siguiente:

```
Initialized amdgpu
```

8. En la salida de `DISPLAY=:0 xrandr -q`, debería ver que tiene 2 pantallas virtuales conectadas:

```
~$ DISPLAY=:0 xrandr -q
Screen 0: minimum 320 x 200, current 3840 x 1080, maximum 16384 x 16384
Virtual connected primary 1920x1080+0+0 (normal left inverted right x axis y axis)
 0mm x 0mm
 4096x3112  60.00
 3656x2664  59.99
 4096x2160  60.00
 3840x2160  60.00
 1920x1200  59.95
 1920x1080  60.00
 1600x1200  59.95
 1680x1050  60.00
 1400x1050  60.00
 1280x1024  59.95
 1440x900 59.99
 1280x960 59.99
 1280x854 59.95
 1280x800 59.96
 1280x720 59.97
 1152x768 59.95
 1024x768 60.00 59.95
 800x600  60.32 59.96 56.25
 848x480  60.00 59.94
 720x480  59.94
 640x480  59.94 59.94
Virtual-1 connected 1920x1080+1920+0 (normal left inverted right x axis y axis) 0mm x
 0mm
 4096x3112  60.00
 3656x2664  59.99
 4096x2160  60.00
 3840x2160  60.00
 1920x1200  59.95
 1920x1080  60.00
 1600x1200  59.95
 1680x1050  60.00
 1400x1050  60.00
```

```
 1280x1024  59.95
 1440x900 59.99
 1280x960 59.99
 1280x854 59.95
 1280x800 59.96
 1280x720 59.97
 1152x768 59.95
 1024x768 60.00 59.95
 800x600  60.32 59.96 56.25
 848x480  60.00 59.94
 720x480  59.94
640x480  59.94 59.94
```

9. Cuando se conecte al DCV, cambie la resolución a 2x4K, confirmando que el DCV registra la compatibilidad con dos monitores.

Introducción a las instancias P5 para Linux

Las instancias P5 proporcionan 8 GPU NVIDIA H100 con 640 GB de memoria de GPU de gran ancho de banda. Cuentan con procesadores AMD EPYC de tercera generación y proporcionan 2 TB de memoria del sistema, 30 TB de almacenamiento de instancias NVMe local, ancho de banda de la red agregado de 3200 Gbps y compatibilidad con RDMA con GPUDirect. Las instancias P5 también admiten la tecnología Amazon EC2 UltraCluster, que proporciona una latencia más baja y un mejor rendimiento de la red mediante EFA.

En la siguiente tabla, se proporciona un resumen de las especificaciones de `p5.48xlarge`.

vCPU	Memoria del sistema	GPU	Memo de GPU	Ancho de banda de red	RDMA con GPUDirect	GPU conexi a conexi	Almacenam iento de la instancia
192	2 TiB	8 GPU NVIDIA H100	640 GI HBM3	3200 Gbps con EFAv2	Compatible	NVSw de 900 GI s	8 volúmenes SSD NVMe de 3800 GB

Configuración de software

La forma más sencilla de empezar con las instancias P5 es iniciar una instancia mediante una AWS Deep Learning AMI que está preconfigurada con todo el software necesario. Para conocer las últimas AWS Deep Learning AMI para su uso con instancias P5, consulte AMI de GPU de base de aprendizaje profundo de AWS (Ubuntu 20.04).

Si necesita crear una AMI personalizada para usarla con instancias P5, le recomendamos que instale las siguientes versiones mínimas de software:

- Controlador NVIDIA 535.54.03 o versiones posteriores
- CUDA 12.1 o versiones posteriores
- NVIDIA GDRCopy 2.3 o versiones posteriores
- Instalador EFA 1.24.1 o versiones posteriores
- NCCL 2.18.3 o versiones posteriores
- complemento aws-ofi-nccl 1.7.2-aws o versiones posteriores

También se recomienda configurar la instancia para que no utilice estados C más profundos. Para obtener más información, consulte High performance and low latency by limiting deeper C-states en la Guía del usuario de Amazon Linux 2. La última AMI de GPU de base de aprendizaje profundo de AWS está preconfigurada para no utilizar estados C más profundos.

Recomendaciones específicas para Ubuntu 20.04

Las siguientes recomendaciones para Ubuntu 20.04 ayudan a evitar que los nombres de las interfaces sean impredecibles durante el arranque:

- Asegúrese de que esté ejecutando `systemd 245.4-4ubuntu3.19` o una versión posterior con el siguiente comando:

```
systemd --version
```

- Asegúrese de haber configurado GRUB:
  - Abra el archivo de configuración `/etc/default/grub` en un editor de texto.
  - Edite la entrada `GRUB_CMDLINE_LINUX_DEFAULT` para incluir `net.naming-scheme=v247`.
  - Reinicie la instancia mediante la ejecución de `sudo update-grub`.

Configuración de redes y EFA

Las instancias P5 ofrecen 3200 Gbps de ancho de banda de la red mediante el uso de varias interfaces EFA. Las instancias P5 admiten 32 tarjetas de red. Le recomendamos que defina una única interfaz de red EFA por tarjeta de red. Para configurar estas interfaces en el momento de la inicialización, recomendamos los siguientes ajustes:

- Para la interfaz de red `0`, especifique el índice de dispositivos `0`.
- Para las interfaces de red de `1` a `31`, especifique el índice de dispositivos `1`.

Para obtener más información acerca de cómo configurar las instancias P5 para EFA, consulte Introducción a las instancias P5 y EFA.

Instancias de Mac de Amazon EC2

Las instancias de Mac de Amazon EC2 admiten de forma nativa el sistema operativo macOS.

- Las instancias x86 de Mac de EC2 (`mac1.metal`) se crean en hardware Mac mini de 2018 con procesadores Intel Core i7 de octava generación (Coffee Lake) de 3.2 GHz.
- Las instancias de Mac M1 de EC2 (`mac2.metal`) se basan en el hardware Mac mini de 2020 y cuentan con procesadores Apple Silicon M1.
- Las instancias de Mac M2 de EC2 (`mac2-m2.metal`) se basan en el hardware Mac mini de 2023 y cuentan con procesadores Apple Silicon M2.
- Las instancias de Mac M2 Pro de EC2 (`mac2-m2pro.metal`) se basan en el hardware Mac mini de 2023 y cuentan con procesadores Apple Silicon M2 Pro.

Las instancias de Mac de EC2 son ideales para desarrollar, crear, probar y firmar aplicaciones para plataformas de Apple, como iPhone, iPad, Mac, Vision Pro, Apple Watch, Apple TV y Safari. Puede conectarse a la instancia Mac mediante SSH o Apple Remote Desktop (ARD).

> **Note**
>
> La unidad de facturación es el host dedicado. Las instancias que se ejecutan en ese host no tienen ningún cargo adicional.

Contenido

Consideraciones

Las siguientes consideraciones se aplican a las instancias Mac:

- Las instancias Mac solo están disponibles como instancias bare metal en hosts dedicados, con un periodo de asignación mínimo de 24 horas antes de que pueda iniciar el host dedicado. Puede iniciar una instancia Mac por host dedicado. Puede compartir el host dedicado con las cuentas de AWS o unidades organizativas de su organización de AWS, o con toda la organización de AWS.
- Las instancias Mac están disponibles en diferentes Regiones de AWS. Para obtener una lista de la disponibilidad de las instancias de Mac en cada una de Regiones de AWS, consulte los tipos de instancias de Amazon EC2 por región.
- Las instancias Mac solo están disponibles como instancias bajo demanda. No están disponibles como instancias de spot o instancias reservadas. Para ahorrar dinero en instancias Mac, puede comprar un Savings Plan.
- Las instancias de Mac pueden ejecutar uno de los siguientes sistemas operativos:
  - macOS Mojave (versión 10.14) (solo instancias de Mac x86)
  - macOS Catalina (versión 10.15) (solo instancias de Mac x86)
  - macOS Big Sur (versión 11) (instancias de Mac x86 y M1)

  - macOS Monterey (versión 12) (instancias de Mac x86 y M1)
  - macOS Ventura (versión 13) (todas las instancias de Mac; las instancias de Mac M2 y M2 Pro son compatibles con macOS Ventura versión 13.2 o posterior)
  - macOS Sonoma (versión 14) (todas las instancias de Mac)
- Se admite la conexión en caliente de EBS.
- AWS no administra ni admite el SSD interno en el hardware de Apple. Le recomendamos encarecidamente que utilice volúmenes de Amazon EBS en su lugar. Los volúmenes de EBS ofrecen las mismas ventajas de elasticidad, disponibilidad y durabilidad en las instancias de Mac que en cualquier otra instancia de EC2.
- Recomendamos el uso de SSD de uso general (`gp2` y `gp3`) y SSD de IOPS aprovisionadas (`io1` y `io2`) con instancias Mac para obtener un óptimo rendimiento de EBS.
- Las instancias de Mac admiten Amazon EC2 Auto Scaling.
- En las instancias de Mac x86, las actualizaciones de software automáticas están desactivadas. Recomendamos aplicar actualizaciones y probarlas en la instancia antes de poner la instancia en producción. Para obtener más información, consulte Actualizar el sistema operativo y el software en las instancias de Mac.
- Cuando detiene o finaliza una instancia de Mac, se realiza un flujo de trabajo de limpieza en el host dedicado. Para obtener más información, consulte Detener y finalizar la instancia de Mac.

> **Warning**
>
> No utilice FileVault. Si habilita FileVault, el host no podrá arrancar debido a que las particiones están bloqueadas. Si se requiere el cifrado de datos, use el cifrado de Amazon EBS para evitar problemas de arranque e impacto en el rendimiento. Con el cifrado de Amazon EBS, las operaciones de cifrado se realizan en los servidores que alojan las instancias, lo que garantiza la seguridad de los datos en reposo y en tránsito entre una instancia y su almacenamiento EBS adjunto. Para obtener más información, consulte Cifrado de Amazon EBS en la Guía del usuario de Amazon EBS.

Preparación de las instancias

Después de iniciar una instancia de Mac, tendrá que esperar a que la instancia esté lista para poder conectarse a ella. Para una AMI distribuida por AWS con una instancia de Mac x86 o una instancia de Mac de Apple Silicon, el tiempo de inicialización puede oscilar entre los 6 y los 20 minutos. En

función de los tamaños de volumen de Amazon EBS elegidos, de la inclusión de scripts adicionales en los datos del usuario o de la carga de software adicional en una AMI de macOS personalizada, el tiempo de inicialización puede aumentar.

Puede usar un pequeño script de shell, como el que se muestra a continuación, para sondear la API describe-instance-status y saber cuándo está lista la instancia para conectarse a ella. En el siguiente comando, sustituya el ID de instancia de ejemplo por el suyo propio.

```
for i in $(seq 1 200); do aws ec2 describe-instance-status --instance-
ids=i-0123456789example \
    --query='InstanceStatuses[0].InstanceStatus.Status'; sleep 5; done;
```

AMI de macOS de EC2

macOS de Amazon EC2 está diseñado para proporcionar un entorno estable, seguro y de alto rendimiento para cargas de trabajo de desarrolladores que se ejecutan en instancias de Mac de Amazon EC2. Las AMI de macOS de EC2 incluyen paquetes que facilitan la integración con AWS, incluidas herramientas de configuración de inicialización y bibliotecas y herramientas populares de AWS.

Para obtener más información sobre AMI de macOS EC2, consulte Notas de la versión de las AMI de macOS de Amazon EC2.

AWS proporciona AMI de macOS EC2 actualizadas de forma regular, que incluyen actualizaciones de paquetes propiedad de AWS y la versión más reciente de macOS completamente probada. Además, AWS proporciona AMI actualizadas con las últimas actualizaciones de versiones secundarias o principales tan pronto como pueden probarse y examinarse completamente.
Si no necesita conservar datos o personalizaciones en las instancias Mac, puede obtener las actualizaciones más recientes mediante el inicio de una nueva instancia con la AMI actual y, a continuación, la finalización de la instancia anterior. De lo contrario, puede elegir qué actualizaciones se aplicarán a las instancias Mac.

Para obtener información acerca de cómo suscribirse a las notificaciones de la AMI de macOS, consulte Suscríbase a las notificaciones de AMI de macOS.

EC2 macOS Init

Init macOS de EC2 se utiliza para inicializar las instancias Mac EC2 en la inicialización. Utiliza grupos de prioridad para ejecutar grupos lógicos de tareas al mismo tiempo.

El archivo launchd plist es `/Library/LaunchDaemons/com.amazon.ec2.macos-init.plist`. Los archivos de EC2 macOS Init se encuentran en `/usr/local/aws/ec2-macos-init`.

Para obtener más información, consulte https://github.com/aws/ec2-macos-init.

Monitor de sistema de Amazon EC2 para macOS

El monitor de sistema de Amazon EC2 para macOS proporciona métricas de utilización de la CPU a Amazon CloudWatch. Envía estas métricas CloudWatch a través de un dispositivo serie personalizado en periodos de 1 minuto. Puede habilitar o deshabilitar este agente de la siguiente manera. Está habilitado de forma predeterminada.

```
sudo setup-ec2monitoring [enable | disable]
```

> **Note**
>
> El monitor de sistema de Amazon EC2 para macOS no es compatible actualmente con las instancias Mac de silicio de Apple.

Recursos relacionados

Para obtener más información acerca de los precios, consulte Precios de .

Para obtener más información acerca de las instancias de Mac, consulte instancias de Mac de Amazon EC2.

Para obtener más información sobre las especificaciones de hardware y el rendimiento de la red de las instancias de Mac, consulte instancias de uso general.

inicialización de una instancia de Mac

Las instancias de Mac de EC2 requieren un host dedicado. Primero debe asignar un host a la cuenta y, a continuación, iniciar la instancia en el host.

Para iniciar una instancia de Mac, use la AWS Management Console o la AWS CLI.

Iniciar una instancia Mac mediante la consola

Para iniciar una instancia Mac en un host dedicado

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. Asigne el host dedicado de la siguiente manera:
   a. En el panel de navegación, seleccione Hosts dedicados.
   b. Elija Allocate Dedicated Host (Asignar host dedicado) y, a continuación, haga lo siguiente:
      i. En Familia de instancias, elija mac1, mac2, mac2-m2 o mac2-m2pro. Si la familia de instancias no aparece en la lista, no se admite en la región seleccionada actualmente.
      ii. En Tipo de instancia, elija mac1.metal, mac2.metal, mac2-m2.metal o mac2-m2pro.metal en función de la familia de instancias elegida.
      iii. En Availability Zone (Zona de disponibilidad), seleccione la zona de disponibilidad para el host dedicado.
      iv. En Quantity (Cantidad), mantenga 1.
      v. Elija Asignar.
3. Lance la instancia en el host de la siguiente manera:
   a. Seleccione el host dedicado que creó y, a continuación, haga lo siguiente:
      i. Elija Acciones, Iniciar instancias en el host.
      ii. En Application and OS Images (Amazon Machine Image) (Imágenes de aplicaciones y sistema operativo [Imagen de máquina de Amazon]), seleccione una AMI de macOS.
      iii. En Tipo de instancia, seleccione el tipo de instancia apropiado (mac1.metal, mac2.metal, mac2-m2.metal o mac2-m2pro.metal).
      iv. En Advanced details (Detalles avanzados), verifique que Tenancy (Tenencia), Tenancy host by (Host de tenencia de) y Tenancy host ID (ID de host de tenencia) estén preconfigurados en función del host dedicado que ha creado. Actualice Tenancy Affinity (Afinidad de tenencia) según sea necesario.
      v. Complete el asistente, especifique volúmenes de EBS, grupos de seguridad y pares de claves según sea necesario.
      vi. En el panel Resumen, elija Iniciar instancia.
   b. Verá una página de confirmación que indicará que la instancia se está iniciando. Elija Ver todas las instancias para cerrar la página de confirmación y volver a la consola. El estado

inicial de una instancia es `pending`. La instancia está lista cuando su estado cambia a `running` y pasa las comprobaciones de estado.

Iniciar una instancia Mac mediante el comando AWS CLI

Asignación del host dedicado

Utilice el comando allocate-hosts para asignar un host dedicado a la instancia de Mac, sustituya `instance-type` por `mac1.metal`, `mac2.metal`, `mac2-m2.metal` o `mac2-m2pro.metal`, así como `region` y `availability-zone` por los valores correctos para su entorno.

```
aws ec2 allocate-hosts --region us-east-1 --instance-type mac1.metal --availability-
zone us-east-1b --auto-placement "on" --quantity 1
```

inicialización de la instancia en el host

Utilice el siguiente comando run-instances para iniciar una instancia de Mac y, de nuevo, reemplace `instance-type` por `mac1.metal`, `mac2.metal`, `mac2-m2.metal` o `mac2-m2pro.metal` y `region` y `availability-zone` por los valores que utilizó en el paso anterior.

```
aws ec2 run-instances --region us-east-1 --instance-type mac1.metal --placement
 Tenancy=host --image-id ami_id --key-name my-key-pair
```

El estado inicial de una instancia es `pending`. La instancia está lista cuando su estado cambia a `running` y pasa las comprobaciones de estado. Utilice el siguiente comando describe-instance-status para mostrar la información de estado de la instancia.

```
aws ec2 describe-instance-status --instance-ids i-017f8354e2dc69c4f
```

A continuación, se muestra un ejemplo de salida de una instancia en ejecución y que ha pasado las comprobaciones de estado.

```
{
    "InstanceStatuses": [
        {
            "AvailabilityZone": "us-east-1b",
            "InstanceId": "i-017f8354e2dc69c4f",
            "InstanceState": {
                "Code": 16,
                "Name": "running"
```

```
            },
            "InstanceStatus": {
                "Details": [
                    {
                        "Name": "reachability",
                        "Status": "passed"
                    }
                ],
                "Status": "ok"
            },
            "SystemStatus": {
                "Details": [
                    {
                        "Name": "reachability",
                        "Status": "passed"
                    }
                ],
                "Status": "ok"
            }
        }
    ]
}
```

Conexión a su instancia de Mac

Puede conectarse a la instancia de Mac mediante SSH o una interfaz gráfica de usuario.

Conéctese a la instancia mediante SSH.

> **Important**
>
> Varios usuarios pueden acceder al sistema operativo simultáneamente. Normalmente, la sesión usuario:GUI es 1:1, debido al servicio Compartir pantalla integrado en el puerto 5900. El uso de SSH en macOS admite varias sesiones, hasta el límite establecido para Max Sessions en el archivo sshd_config.

Las instancias de Mac de Amazon EC2 no permiten el SSH raíz remoto de forma predeterminada. La autenticación de contraseñas se deshabilita para evitar ataques de contraseña a la fuerza. La cuenta ec2-user está configurada para iniciar sesión de manera remota mediante SSH. La cuenta ec2-user también tiene privilegios sudo. Después de conectarse a la instancia, puede agregar otros usuarios.

Para admitir la conexión a la instancia mediante SSH, inicie la instancia con un par de claves y un grupo de seguridad que permita el acceso SSH y asegúrese de que la instancia tenga conectividad a Internet. Cuando se conecta a la instancia, proporciona el `.pem` archivo para el par de claves.

Para conectarse a la instancia Mac mediante un cliente SSH, use el siguiente procedimiento. Si aparece un error al intentar conectarse a la instancia, consulte Solución de problemas de conexión a la instancia de Linux.

Para conectarse a la instancia mediante SSH

1. ingrese ssh en la línea de comandos, a fin de comprobar que el equipo local tiene instalado un cliente SSH. Si el equipo no reconoce el comando, busque un cliente SSH para el sistema operativo e instálelo.
2. Obtenga el nombre DNS público de la instancia. Mediante la Amazon EC2 consola, puede encontrar el nombre DNS público en las fichas Detalles yRedes. Mediante el AWS CLI, puede encontrar el nombre DNS público con el comando describe-instances.
3. Localice el `.pem` archivo para el par de claves que especificó cuando inició la instancia.
4. Conéctese a la instancia mediante el siguiente ssh comando y especifique el nombre DNS público de la instancia y el `.pem` archivo.

```
ssh -i /path/key-pair-name.pem ec2-user@instance-public-dns-name
```

Conéctese a la interfaz gráfica de usuario (GUI) de la instancia

Siga el siguiente procedimiento para conectarse a la GUI de su instancia mediante VNC, Apple Remote Desktop (ARD) o la aplicación Apple Screen Sharing (que se incluye en macOS).

> **Note**
>
> macOS 10.14 y versiones posteriores solo permite el control si el Uso compartido de pantalla está habilitado a través de System Preferences (Preferencias del sistema).

Para conectarse a la instancia mediante un cliente de ARD o VNC

1. Compruebe que el equipo local tiene instalado un cliente ARD o un cliente VNC compatible con ARD. En macOS, puede aprovechar la aplicación integrada para compartir pantalla. De lo contrario, busque ARD para su sistema operativo e instálelo.

2. Desde el equipo local, conéctese a la instancia mediante SSH.
3. Configure una contraseña para la cuenta ec2-user de la siguiente manera, mediante el comando passwd.

```
[ec2-user ~]$ sudo passwd ec2-user
```

4. Instale e inicie Compartir pantalla de macOS con el siguiente comando.

```
[ec2-user ~]$ sudo launchctl enable system/com.apple.screensharing
sudo launchctl load -w /System/Library/LaunchDaemons/com.apple.screensharing.plist
```

5. Para desconectarse de la instancia, ingrese exit y presione Entrar.
6. Desde el equipo, conéctese a la instancia mediante el siguiente ssh comando. Además de las opciones mostradas en la sección anterior, utilice la opción -L para habilitar el reenvío de puertos y reenviar todo el tráfico del puerto local 5900 al servidor ARD de la instancia.

```
ssh -L 5900:localhost:5900 -i /path/key-pair-name.pem ec2-user@instance-public-dns-name
```

7. Desde el equipo local, utilice el cliente de ARD o de VNC que admita ARD para conectarse a `localhost:5900`. Por ejemplo, utilice la aplicación Compartir pantalla en macOS de la siguiente manera:
   a. Abra Finder y seleccione Ir.
   b. Seleccione Conectarse a un servidor.
   c. En el campo Dirección del servidor, introduzca `vnc://localhost:5900`.
   d. Inicie sesión de la manera indicada y utilice **`ec2-user`** como nombre de usuario y la contraseña que creó para la cuenta ec2-user.

Modificar la resolución de pantalla de macOS en instancias Mac

Una vez que se conecte a su instancia de Mac de EC2 mediante ARD o un cliente VNC compatible con ARD, puede modificar la resolución de pantalla de su entorno macOS a través de cualquiera de las herramientas o utilidades de macOS disponibles de forma pública, como displayplacer.

Para modificar la resolución de pantalla mediante displayplacer

1. Instale displayplacer.

```
[ec2-user ~]$ brew tap jakehilborn/jakehilborn && brew install displayplacer
```

2. Muestre la información de pantalla actual y posibles resoluciones de pantalla.

```
[ec2-user ~]$ displayplacer list
```

3. Aplique la resolución de pantalla deseada.

```
[ec2-user ~]$ displayplacer "id:<screenID> res:<width>x<height> origin:(0,0)
 degree:0"
```

Por ejemplo:

```
RES="2560x1600"
displayplacer "id:69784AF1-CD7D-B79B-E5D4-60D937407F68 res:${RES} scaling:off
 origin:(0,0) degree:0"
```

Actualizar el sistema operativo y el software en las instancias de Mac

Warning

La instalación de las versiones beta o preliminar de macOS solo está disponible en las instancias Mac de Amazon EC2 M1. Amazon EC2 no califica las versiones beta ni las versiones preliminares de macOS y no garantiza que las instancias sigan funcionando después de actualizar una versión de macOS en preproducción.
Intentar instalar versiones beta o ver versiones preliminares de macOS en instancias de Mac Amazon EC2 x86 conducirá a la degradación de su host dedicado Amazon EC2 Mac cuando detenga o finalice sus instancias, y le impedirá iniciar o iniciar una nueva instancia en ese host.

Pasos para actualizar el software en instancias de Mac x86 e instancias de Mac de Apple Silicon.

- Actualización del software en instancias x86 de Mac
- Actualización del software en instancias de Mac de Apple Silicon

Actualización del software en instancias x86 de Mac

En las instancias de Mac x86, puede instalar actualizaciones del sistema operativo desde Apple mediante el comando `softwareupdate`.

Para instalar actualizaciones del sistema operativo desde Apple en instancias de Mac x86

1. Enumere los paquetes con actualizaciones disponibles mediante el siguiente comando.

   ```
   [ec2-user ~]$ softwareupdate --list
   ```

2. Instale todas las actualizaciones o solo actualizaciones específicas. Para instalar actualizaciones específicas, utilice el siguiente comando.

   ```
   [ec2-user ~]$ sudo softwareupdate --install label
   ```

   De lo contrario, para instalar todas las actualizaciones, utilice el siguiente comando.

   ```
   [ec2-user ~]$ sudo softwareupdate --install --all --restart
   ```

Los administradores del sistema pueden utilizar AWS Systems Manager para implementar actualizaciones preaprobadas en instancias Mac x86. Para obtener más información, consulte la Guía del usuario de AWS Systems Manager.

Puede utilizar Homebrew para instalar actualizaciones de paquetes en las AMI de macOS EC2, a fin de tener la versión más reciente de estos paquetes en sus instancias. También puede utilizar Homebrew para instalar y ejecutar aplicaciones macOS comunes en Amazon EC2 macOS. Para obtener más información, consulte la Documentación de Homebrew.

Para instalar actualizaciones con Homebrew, haga lo siguiente:

1. Actualice Homebrew mediante el siguiente comando.

   ```
   [ec2-user ~]$ brew update
   ```

2. Enumere los paquetes con actualizaciones disponibles mediante el siguiente comando.

   ```
   [ec2-user ~]$ brew outdated
   ```

3. Instale todas las actualizaciones o solo actualizaciones específicas. Para instalar actualizaciones específicas, utilice el siguiente comando.

```
[ec2-user ~]$ brew upgrade package name
```

De lo contrario, para instalar todas las actualizaciones, utilice el siguiente comando.

```
[ec2-user ~]$ brew upgrade
```

Actualización del software en instancias de Mac de Apple Silicon

Consideraciones

Controlador Elastic Network Adapter (ENA)

Debido a una actualización en la configuración del controlador de red, la versión 1.0.2 del controlador ENA no es compatible con macOS 13.3 o superior. Si quieres instalar una nueva versión de macOS de, versión 13.3 o posterior, siga el procedimiento que se explica a continuación para instalar una nueva versión del controlador.

Para instalar una nueva versión del controlador ENA

1. En una ventana del terminal, conéctese a la instancia de Mac de Apple Silicon mediante SSH.
2. Descargue la aplicación ENA en el archivo `Applications` con el siguiente comando:

```
[ec2-user ~]$ brew install amazon-ena-ethernet-dext
```

> **Consejo para la solución de problemas**
>
> Si recibe la advertencia `No available formula with the name amazon-ena-ethernet-dext`, ejecute el siguiente comando:
>
> ```
> [ec2-user ~]$ brew update
> ```

3. Para desconectarse de la instancia, ingrese exit y presione Entrar.
4. Utilice el cliente de VNC para activar la aplicación ENA.

a. Configure el cliente de VNC mediante Conéctese a la interfaz gráfica de usuario (GUI) de la instancia.
b. Una vez que se haya conectado a la instancia mediante la aplicación de uso compartido de pantalla, vaya a la carpeta Aplicaciones y abra la aplicación ENA.
c. Elija Activar.
d. Para confirmar que el controlador se activó correctamente, ejecute el siguiente comando en la ventana del terminal. El resultado del comando muestra que el controlador antiguo está en el estado de finalización y el nuevo controlador está en el estado activado.

```
systemextensionsctl list;
```

e. Tras reiniciar la instancia, solo estará presente el nuevo controlador.

Actualización de software en instancias de Mac de Apple Silicon

En las instancias de Mac de Apple Silicon, debe completar varios pasos para actualizar el sistema operativo de forma local. Primero, acceda al disco interno de la instancia mediante la GUI con un cliente VNC (Computación virtual en red). Este procedimiento utiliza Compartir pantalla de macOS, el cliente VNC integrado. A continuación, delegue la propiedad al usuario administrativo (`ec2-user`); para ello, inicie sesión como `aws-managed-user` en el volumen de Amazon EBS.

Al realizar este procedimiento, creará dos contraseñas. Una contraseña es para el usuario administrativo (`ec2-user`) y la otra para un usuario administrativo especial (`aws-managed-user`). Recuerde estas contraseñas, ya que las utilizará a medida que avance en el procedimiento.

> **Note**
>
> Con este procedimiento en macOS Big Sur, solo puede realizar actualizaciones menores, como la actualización de macOS Big Sur 11.7.3 a macOS Big Sur 11.7.4. Para macOS Monterey o superior, puede hacer actualizaciones de software importantes.

Para acceder al disco interno

1. Desde el equipo local, en el terminal, conéctese a la instancia de Mac de Apple Silicon mediante SSH con el siguiente comando. Para obtener más información, consulte Conéctese a la instancia mediante SSH..

```
ssh -i /path/key-pair-name.pem ec2-user@instance-public-dns-name
```

2. Instale e inicie Compartir pantalla de macOS con el siguiente comando.

```
[ec2-user ~]$ sudo launchctl enable system/com.apple.screensharing
sudo launchctl load -w /System/Library/LaunchDaemons/com.apple.screensharing.plist
```

3. Establezca una contraseña para `ec2-user` con el comando siguiente. Recuerde la contraseña, ya que la usará más adelante.

```
[ec2-user ~]$ sudo /usr/bin/dscl . -passwd /Users/ec2-user
```

4. Para desconectarse de la instancia, escriba exit y presione return.
5. Desde su equipo local, en el terminal, vuelva a conectarse a la instancia mediante un túnel de SSH al puerto VNC mediante el siguiente comando.

```
ssh -i /path/key-pair-name.pem -L 5900:localhost:5900 ec2-user@instance-public-dns-name
```

> **Note**
>
> No salga de esta sesión de SSH hasta que se hayan completado los siguientes pasos de conexión de la VNC y GUI. Cuando se reinicie la instancia, la conexión se cerrará automáticamente.

6. En el equipo local, conéctese a `localhost:5900` mediante los siguientes pasos:
   a. Abra Finder y seleccione Ir.
   b. Seleccione Conectarse a un servidor.
   c. En el campo Dirección del servidor, introduzca `vnc://localhost:5900`.
7. En la ventana de macOS, conéctese a la sesión remota de la instancia de Mac de Apple Silicon como `ec2-user` con la contraseña que creó en el paso 3.
8. Acceda al disco interno, denominado InternalDisk, mediante una de las siguientes opciones.
   a. Para macOS Ventura o superior: abra Ajustes del sistema, seleccione General en el panel izquierdo y Disco de arranque en la esquina inferior derecha del panel.

b. Para macOS Monterey o versiones anteriores: abra Ajustes del sistema, seleccione Disco de arranque y, a continuación, desbloquee el panel; para ello, debe seleccionar el icono del candado en la esquina inferior izquierda de la ventana.

> **Consejo para la solución de problemas**
>
> Si necesita montar el disco interno, ejecute el siguiente comando en el terminal.
>
> ```
> APFSVolumeName="InternalDisk" ; SSDContainer=$(diskutil list | grep
>  "Physical Store disk0" -B 3 | grep "/dev/disk" | awk {'print $1'} ) ;
>  diskutil apfs addVolume $SSDContainer APFS $APFSVolumeName
> ```

9. Elija el disco interno, denominado InternalDisk, y seleccione Reiniciar. Seleccione Reiniciar de nuevo cuando se le solicite.

> **Important**
>
> Si el disco interno se denomina Macintosh HD en lugar de InternalDisk, es necesario detener y reiniciar la instancia para poder actualizar el host dedicado. Para obtener más información, consulte Detener y finalizar la instancia de Mac.

Utilice el siguiente procedimiento para delegar la propiedad al usuario administrativo. Cuando vuelva a conectarse a la instancia con SSH, arranque desde el disco interno mediante el usuario administrativo especial (`aws-managed-user`). La contraseña inicial de `aws-managed-user` está en blanco, por lo que tendrá que sobrescribirla en su primera conexión. A continuación, debe repetir los pasos para instalar e iniciar Compartir pantalla de macOS, ya que el volumen de arranque ha cambiado.

Para delegar la propiedad al administrador de un volumen de Amazon EBS

1. Desde el equipo local, en el terminal, conéctese a la instancia de Mac Apple Silicon mediante el siguiente comando.

```
ssh -i /path/key-pair-name.pem aws-managed-user@instance-public-dns-name
```

2. Cuando reciba la advertencia `WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!`, utilice uno de los siguientes comandos para resolver el problema.

   a. Elimine los hosts conocidos mediante el siguiente comando. A continuación, repita el paso anterior.

   ```
   rm ~/.ssh/known_hosts
   ```

   b. Agregue lo siguiente al comando SSH del paso anterior.

   ```
   -o UserKnownHostsFile=/dev/null -o StrictHostKeyChecking=no
   ```

3. Establezca la contraseña para `aws-managed-user` con el siguiente comando. La contraseña inicial de `aws-managed-user` está en blanco, por lo que debe sobrescribirla en su primera conexión.

   a.
   ```
   [aws-managed-user ~]$ sudo /usr/bin/dscl . -passwd /Users/aws-managed-
   user password
   ```

   b. Cuando reciba el mensaje `Permission denied. Please enter user's old password:`, pulse Entrar.

   > **Consejo para la solución de problemas**
   >
   > Si aparece el error `passwd: DS error: eDSAuthFailed`, utilice el siguiente comando.
   >
   > ```
   > [aws-managed-user ~]$ sudo passwd aws-managed-user
   > ```

4. Instale e inicie Compartir pantalla de macOS con el siguiente comando.

   ```
   [aws-managed-user ~]$ sudo launchctl enable system/com.apple.screensharing
   sudo launchctl load -w /System/Library/LaunchDaemons/com.apple.screensharing.plist
   ```

5. Para desconectarse de la instancia, escriba exit y presione return.

6. Desde su equipo local, en el terminal, vuelva a conectarse a la instancia mediante un túnel de SSH al puerto VNC mediante el siguiente comando.

```
ssh -i /path/key-pair-name.pem -L 5900:localhost:5900 aws-managed-user@instance-public-dns-name
```

7. En el equipo local, conéctese a `localhost:5900` mediante los siguientes pasos:

   a. Abra Finder y seleccione Ir.

   b. Seleccione Conectarse a un servidor.

   c. En el campo Dirección del servidor, introduzca `vnc://localhost:5900`.

8. En la ventana de macOS, conéctese a la sesión remota de la instancia de Mac de Apple Silicon como `aws-managed-user` con la contraseña que creó en el paso 3.

> **Note**
>
> Cuando se le pida que inicie sesión con su ID de Apple, seleccione Configurar más tarde.

9. Acceda al volumen de Amazon EBS mediante una de las siguientes opciones.

   a. Para macOS Ventura o posterior: abra Ajustes del sistema, seleccione General en el panel izquierdo y Disco de arranque en la esquina inferior derecha del panel.

   b. Para macOS Monterey o versiones anteriores: abra Ajustes del sistema, seleccione Disco de arranque y desbloquee el panel al seleccionar el ícono del candado en la esquina inferior izquierda de la ventana.

> **Note**
>
> Hasta que se reinicie, cuando se le solicite una contraseña de administrador, utilice la contraseña que estableció anteriormente para `aws-managed-user`. Esta contraseña puede ser diferente de la que configuró para `ec2-user` o la cuenta de administrador predeterminada de su instancia. Las siguientes instrucciones especifican cuándo usar la contraseña de administrador de la instancia.

10. Seleccione el volumen de Amazon EBS (el volumen que no se denomina InternalDisk en la ventana Disco de arranque) y elija Reiniciar.

> **Note**
>
> Si tiene varios volúmenes de Amazon EBS de arranque adjuntos a la instancia de Mac de Apple Silicon, asegúrese de utilizar un nombre único para cada volumen.

11. Confirme el reinicio y, a continuación, seleccione Autorizar usuarios cuando se le solicite.
12. En el panel Autorizar usuario en este volumen, compruebe que el usuario administrativo (de manera predeterminada `ec2-user`) esté seleccionado y, después, seleccione Autorizar.
13. Ingrese la contraseña de `ec2-user` que creó en el paso 3 del procedimiento anterior y, luego, seleccione Continuar.
14. Ingrese la contraseña del usuario administrativo especial (`aws-managed-user`) cuando se le solicite.
15. En el equipo local, en el terminal, vuelva a conectarse a la instancia mediante SSH con el nombre de usuario `ec2-user`.

> **Consejo para la solución de problemas**
>
> Si recibe la advertencia `WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!`, ejecute el siguiente comando y vuelva a conectarse a la instancia mediante SSH.
>
> ```
> rm ~/.ssh/known_hosts
> ```

16. Para realizar la actualización del software, utilice los siguientes comandos en Actualización del software en instancias x86 de Mac.

Aumente el tamaño de un volumen de EBS en la instancia Mac

Puede aumentar el tamaño de los volúmenes Amazon EBS en la instancia Mac. Para obtener más información, consulte Volúmenes elásticos de Amazon EBS en la Guía del usuario de Amazon EBS.

Después de aumentar el tamaño del volumen, debe aumentar el tamaño del contenedor APFS de la siguiente manera.

Aumente el espacio en disco disponible para su uso

1. Determine si es necesario reiniciar. Si cambia el tamaño de un volumen de EBS existente en una instancia Mac en ejecución, debe reiniciar la instancia para que el tamaño nuevo esté disponible. Si la modificación del espacio en disco se hizo durante la inicialización, no será obligatorio llevar a cabo el reinicio.

   Consulte el estado actual de los tamaños de disco:

   ```
   [ec2-user ~]$  diskutil list external physical
   /dev/disk0 (external, physical):
      #:                       TYPE NAME                    SIZE       IDENTIFIER
      0:                 GUID_partition_scheme            *322.1 GB     disk0
      1:                 EFI EFI                           209.7 MB     disk0s1
      2:                 Apple_APFS Container disk2        321.9 GB     disk0s2
   ```

2. Copie y pegue el siguiente comando.

   ```
   [ec2-user ~]$ PDISK=$(diskutil list physical external | head -n1 | cut -d" " -f1)
   APFSCONT=$(diskutil list physical external | grep "Apple_APFS" | tr -s " " | cut -
   d" " -f8)
   yes | sudo diskutil repairDisk $PDISK
   ```

3. Copie y pegue el siguiente comando.

   ```
   [ec2-user ~]$ sudo diskutil apfs resizeContainer $APFSCONT 0
   ```

Detener y finalizar la instancia de Mac

Cuando detiene una instancia Mac, la instancia permanece en el estado `stopping` durante unos 15 minutos antes de pasar al estado `stopped`.

Cuando detiene o finaliza una instancia de Mac, Amazon EC2 realiza un flujo de trabajo de limpieza en el host dedicado subyacente para borrar el SSD interno, borrar las variables NVRAM persistentes y actualizar al firmware más reciente del dispositivo. Esto garantiza que las instancias de Mac proporcionen la misma seguridad y privacidad de datos que otras instancias de Nitro EC2. También le permite ejecutar las AMI de macOS más recientes. Durante el flujo de trabajo de limpieza, el host dedicado entra temporalmente en el estado pendiente. En las instancias de Mac x86, el flujo de trabajo de limpieza puede tardar hasta 50 minutos en completarse. En las instancias de Apple Silicon

Mac, el flujo de trabajo de limpieza puede tardar hasta 110 minutos en completarse. Además, en las instancias de Mac x86, si es necesario actualizar el firmware del dispositivo, el flujo de trabajo de limpieza puede tardar hasta 3 horas en completarse.

No puede iniciar la instancia de Mac detenida ni iniciar una nueva instancia de Mac hasta que finalice el flujo de trabajo de limpieza, momento en el que host dedicado entra en el estado `available`.

La medición y la facturación se pausan cuando el host dedicado entra en el estado `pending`. No se le cobrará por la duración del flujo de trabajo de limpieza.

Libere el host dedicado para la instancia Mac

Cuando haya terminado con la instancia Mac, puede liberar el host dedicado. Antes de poder liberar el host dedicado, debe detener o finalizar la instancia Mac. No puede liberar el host hasta que el periodo de asignación supere el mínimo de 24 horas.

Para liberar el host dedicado

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Seleccione la instancia y elija Estado de instancia y, a continuación, elija Detener instancia o Terminar instancia.
4. En el panel de navegación, seleccione Dedicated Hosts (Alojamientos dedicados).
5. Seleccione el host dedicado y elija Acciones, Liberar host.
6. Cuando se le pida que confirme, elija Liberar.

Encuentre versiones de macOS compatibles para su host dedicado de Mac de Amazon EC2

Puede ver las versiones más recientes de macOS compatibles con su host dedicado de Mac de Amazon EC2. Con esta funcionalidad, puede validar si su host dedicado admite la inicialización de instancias con sus versiones de macOS preferidas.

Cada versión de macOS requiere una versión mínima de firmware en el Apple Mac subyacente para arrancar correctamente. La versión del firmware de Apple Mac puede quedar desactualizada si un host dedicado de Mac asignado ha permanecido inactivo durante un período prolongado o si tiene una instancia de larga ejecución.

Para garantizar la compatibilidad con las versiones más recientes de macOS, puede detener o finalizar las instancias en el host dedicado de Mac asignado. Esto activa el flujo de trabajo de limpieza del host y actualiza el firmware del Apple Mac subyacente para que sea compatible con las versiones más recientes de macOS. Un host dedicado con una instancia de larga ejecución se actualizará automáticamente cuando detenga o finalice una instancia en ejecución.

Para obtener más información acerca del flujo de trabajo de limpieza, consulte Detener y finalizar la instancia de Mac.

Para obtener más información acerca de cómo iniciar instancias de Mac, consulte inicialización de una instancia de Mac.

Puede consultar la información sobre las últimas versiones de macOS compatibles con el host dedicado asignado mediante la consola de Amazon EC2 o la AWS CLI.

Console

Para ver la información del firmware del host dedicado mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Hosts dedicados.
3. En la página Información de los hosts dedicados, en Últimas versiones de macOS compatibles, puede consultar las versiones de macOS más recientes compatibles con el host.

AWS CLI

Para ver la información del firmware del host dedicado mediante AWS CLI

Utilice el comando `describe-mac-hosts` y sustituya la `region` por la Región de AWS correspondiente.

```
$ aws ec2 describe-mac-hosts --region us-east-1
  {
      "MacHosts": [
          {
              "HostId": "h-07879acf49EXAMPLE",
              "MacOSLatestSupportedVersions": [
                  "14.3",
                  "13.6.4",
```

```
                "12.7.3"
            ]
        }
    ]
}
```

Suscríbase a las notificaciones de AMI de macOS

Para recibir notificaciones cuando se publiquen nuevas AMI o cuando se haya actualizado bridgeOS, suscríbase mediante Amazon SNS.

Para obtener más información sobre EC2 de macOS, consulte Notas de la versión de las AMI de macOS de Amazon EC2.

Para suscribirse a las notificaciones de AMI de macOS

1. Abra la consola de Amazon SNS en https://console.aws.amazon.com/sns/v3/home.
2. En la barra de navegación, cambie la región a EE. UU. Este (Norte de Virginia), si es necesario. Debe utilizar esta región porque las notificaciones de SNS a las que se va a suscribir se han creado en esta región.
3. En el panel de navegación, seleccione Subscriptions.
4. Seleccione Create subscription.
5. En el cuadro de diálogo Crear suscripción, haga lo siguiente:

   a. En ARN de tema, copie y pegue uno de los siguientes nombres de recursos de Amazon (ARN):

      - **arn:aws:sns:us-east-1:898855652048:amazon-ec2-macos-ami-updates**
      - **arn:aws:sns:us-east-1:898855652048:amazon-ec2-bridgeos-updates**

   b. En Protocolo, seleccione una de las siguientes opciones:

      - Email:

        En Punto de conexión, escriba una dirección de correo electrónico que pueda utilizar para recibir notificaciones. Una vez creada la suscripción, recibirá un mensaje de confirmación con el asunto `AWS Notification - Subscription Confirmation`. Abra el email y elija Confirmar suscripción para completar su suscripción.
      - SMS:

En Punto de conexión, escriba un número de teléfono que pueda utilizar para recibir notificaciones.

- AWS Lambda, Amazon SQS, Amazon Data Firehose (las notificaciones estarán en formato JSON):

  En Punto de conexión, ingrese el ARN de la función de Lambda, la cola de SQS o la secuencia de Firehose que puede utilizar para recibir notificaciones.

c. Seleccione Crear suscripción.

Cuando se publican AMI de macOS, enviamos notificaciones a los suscriptores del tema `amazon-ec2-macos-ami-updates`. Cada vez que se actualiza bridgeOS, enviamos notificaciones a los suscriptores del tema `amazon-ec2-bridgeos-updates`. Si ya no desea recibir estas notificaciones, utilice el siguiente procedimiento para cancelar la suscripción.

Para cancelar la suscripción a las notificaciones de AMI de macOS

1. Abra la consola de Amazon SNS en https://console.aws.amazon.com/sns/v3/home.
2. En la barra de navegación, cambie la región a EE. UU. Este (Norte de Virginia), si es necesario. Debe utilizar esta región porque las notificaciones de SNS se han creado en esa región.
3. En el panel de navegación, seleccione Subscriptions.
4. Seleccione las suscripciones y, a continuación, elija Actions (Acciones), Delete subscriptions (Eliminar suscripciones). Cuando se le pida confirmación, seleccione Delete (Eliminar).

Notas de la versión de las AMI de macOS de Amazon EC2

La siguiente información proporciona detalles sobre los paquetes incluidos de forma predeterminada en las AMI de macOS de EC2 y resume los cambios de cada versión de las AMI de macOS de EC2.

Para obtener información acerca de cómo suscribirse a las notificaciones de la AMI de macOS, consulte Suscríbase a las notificaciones de AMI de macOS.

Paquetes predeterminados incluidos en las AMI de macOS de Amazon EC2

En la siguiente tabla se describen los paquetes que se incluyen de forma predeterminada en las AMI de macOS de EC2.

Paquetes	Notas de la versión
EC2 macOS Init	https://github.com/aws/ec2-macos-init/tags
EC2 macOS Utils	https://github.com/aws/ec2-macos-utils/tags
Amazon SSM Agent	https://github.com/aws/amazon-ssm-agent/releases
AWS Command Line Interface (AWS CLI), versión 2	https://raw.githubusercontent.com/aws/aws-cli/v2/CHANGELOG.rst
Herramientas de línea de comandos para Xcode	https://developer.apple.com/documentation/xcode-release-notes
Homebrew	https://github.com/Homebrew/brew/releases
Conexión de instancia de EC2	https://github.com/aws/aws-ec2-instance-connect-config/releases
Safari	https://developer.apple.com/documentation/safari-release-notes

Actualizaciones de la AMI de macOS de Amazon EC2

En la siguiente tabla se describen los cambios incluidos en las versiones de las AMI de EC2 para macOS. Tenga en cuenta que algunos cambios se aplican a todas las AMI de macOS de EC2, mientras que otros sólo se aplican a un subconjunto de estas AMI.

Actualizaciones de la AMI de macOS de EC2

Versión	Cambios
07/06/2024	Todas las AMI • Se actualizó Homebrew a la versión 4.3.1-1 • Se actualizó `aws-cli` a la versión 2.15.56 • Se actualizó `amazon-ssm-agent` a la versión 3.3.380.0-1

Versión	Cambios

	Versión de macOS Sonoma 14.5 (todas las instancias de Mac)
	• Contenido de seguridad de macOS Sonoma 14.5
	
	Lanzamiento de macOS Ventura 13.6.7 (todas las instancias de Mac)
	• Contenido de seguridad de macOS Ventura 13.6.7
	• Se actualizó Safari a la versión 17.5
	  • Contenido de seguridad de Safari 17.5
	
	Versión de macOS Monterey 12.7.5 (todas las instancias de Mac)
	• Contenido de seguridad de macOS Monterey 12.7.5
	• Se actualizó Safari a la versión 17.5
	  • Contenido de seguridad de Safari 17.5

Versión	Cambios

12/04/2024	Todas las AMI
	• Se actualizó Homebrew a la versión 4.2.16-1
	• Se actualizó `aws-cli` a la versión 2.15.36
	
	Lanzamiento de macOS Sonoma 14.4.1 (todas las instancias de Mac)
	• Contenido de seguridad de macOS Sonoma 14.4.1
	
	Lanzamiento de macOS Ventura 13.6.6 (todas las instancias de Mac)
	• Contenido de seguridad de macOS Ventura 13.6.6
	• Se actualizó Safari a la versión 17.4.1
	  • Contenido de seguridad de Safari 17.4.1
	
	Para macOS Monterey (todas las instancias de Mac)
	• Se actualizó Safari a la versión 17.4.1
	  • Contenido de seguridad de Safari 17.4.1

Instancias optimizadas para Amazon EBS

Una instancia optimizada para Amazon EBS utiliza una pila de configuración optimizada y proporciona capacidad adicional y dedicada para las E/S de Amazon EBS. Esta optimización proporciona el mejor rendimiento para sus volúmenes de EBS, ya que reduce al mínimo la contención entre las E/S de Amazon EBS y otro tráfico procedente de la instancia.

Las instancias optimizadas para EBS proporcionan ancho de banda dedicado para Amazon EBS. Cuando se adjuntan a una instancia optimizada para EBS, los volúmenes de SSD de uso general (`gp2` y `gp3`) están diseñados para ofrecer, al menos, el 90 % de su rendimiento de IOPS aprovisionadas el 99 % del tiempo en un año determinado, mientras que los volúmenes de SSD de IOPS aprovisionadas (`io1` y `io2`) están diseñados para ofrecer, al menos, el 90 % de su rendimiento de IOPS aprovisionadas el 99,9 % del tiempo de un año determinado. Tanto los volúmenes de HDD con rendimiento optimizado (`st1`) como los volúmenes HDD en frío (`sc1`) ofrecen un rendimiento del

90 % de su rendimiento esperado el 99 % del tiempo en un año determinado. Los periodos que no cumplen estas convenciones están distribuidos de manera prácticamente uniforme, alcanzándose el 99 % del rendimiento total previsto cada hora. Para obtener más información, consulte Tipos de volúmenes de Amazon EBS en la Guía del usuario de Amazon EBS.

> **Important**
>
> El rendimiento de EBS de una instancia está limitado por los límites de rendimiento de la instancia o por el rendimiento agregado de sus volúmenes adjuntos, lo que sea menor. Para lograr el máximo rendimiento de EBS, una instancia debe tener volúmenes adjuntos que proporcionen un rendimiento combinado igual o superior al rendimiento máximo de la instancia. Por ejemplo, para alcanzar `80,000` IOPS para `r6i.16xlarge`, la instancia debe tener al menos `5` `gp3` volúmenes aprovisionados con `16,000` IOPS cada uno (`5` volúmenes x `16,000` IOPS = `80,000` IOPS).

Contenido

Tipos de instancias admitidos

En las tablas siguientes se indican los tipos de instancias que admiten la optimización de EBS. Se incluye el ancho de banda dedicado a Amazon EBS, el rendimiento máximo típico que se puede alcanzar en esa conexión con una carga de trabajo de lectura en streaming y tamaño de E/S de 128 KiB y el número máximo de IOPS que admite la instancia si se usa un tamaño de E/S de 16 KiB.

Elija una instancia optimizada para EBS que proporcione más rendimiento dedicado de Amazon EBS del que necesita la aplicación; de no hacerlo así, la conexión entre Amazon EBS y Amazon EC2 puede convertirse en un cuello de botella de rendimiento.

Contenido

- Optimización de EBS admitida

EBS optimizado de forma predeterminada

En la siguiente tabla se enumeran los tipos de instancia que admiten la optimización de EBS, en las que está habilitada de forma predeterminada. No es necesario habilitar la optimización para EBS, ni se produce ningún efecto si la deshabilita.

> **Note**
>
> También puede ver esta información mediante programación con la AWS CLI. Para obtener más información, consulte Ver los tipos de instancias que admiten la optimización de EBS.

Temas

- Fin general
- Optimizada para computación
- Optimizada para memoria
- Optimizada para almacenamiento
- Computación acelerada
- Computación de alto rendimiento

Fin general

> **Important**
>
> [1] Estas instancias pueden ofrecer el máximo rendimiento durante 30 minutos al menos una vez cada 24 horas, tras lo cual vuelven a su rendimiento básico.
> [2] Estas instancias pueden mantener el rendimiento indicado de forma indefinida. Si la carga de trabajo requiere un rendimiento máximo prolongado de más de 30 minutos, utilice una de estas instancias.

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
a1.medium [1]	300	3500	37,50	437,50	2 500	20000
a1.large [1]	525	3500	65,62	437,50	4000	20000
a1.xlarge [1]	800	3500	100,00	437,50	6000	20000
a1.2xlarge [1]	1750	3500	218,75	437,50	10000	20000
a1.4xlarge [2]	3500		437,5		20000	
a1.metal [2]	3500		437,5		20000	
m4.large [2]	450		56,25		3600	
m4.xlarge [2]	750		93,75		6000	
m4.2xlarge [2]	1 000		125,0		8000	
m4.4xlarge [2]	2000		250,0		16 000	
m4.10xlarge [2]	4000		500,0		32 000	
m4.16xlarge [2]	10000		1250,0		65 000	
m5.large [1]	650	4750	81,25	593,75	3600	18 750
m5.xlarge [1]	1150	4750	143,75	593,75	6000	18 750

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
m5.2xlarge [1]	2300	4750	287,50	593,75	12 000	18 750
m5.4xlarge [2]	4750		593,75		18 750	
m5.8xlarge [2]	6800		850,0		30000	
m5.12xlarge [2]	9500		1187.5		40000	
m5.16xlarge [2]	13600		1700,0		60 000	
m5.24xlarge [2]	19 000		2375,0		80 000	
m5.metal [2]	19 000		2375,0		80 000	
m5a.large [1]	650	2 880	81,25	360,00	3600	16 000
m5a.xlarge [1]	1085	2 880	135,62	360,00	6000	16 000
m5a.2xlarge [1]	1580	2 880	197,50	360,00	8333	16 000
m5a.4xlarge [2]	2 880		360,0		16 000	

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
m5a.8xlarge [2]	4750		593,75		20000	
m5a.12xlarge [2]	6780		847,5		30000	
m5a.16xlarge [2]	9500		1187.5		40000	
m5a.24xlarge [2]	13 750		1718,75		60 000	
m5ad.large [1]	650	2 880	81,25	360,00	3600	16 000
m5ad.xlarge [1]	1085	2 880	135,62	360,00	6000	16 000
m5ad.2xlarge [1]	1580	2 880	197,50	360,00	8333	16 000
m5ad.4xlarge [2]	2 880		360,0		16 000	
m5ad.8xlarge [2]	4750		593,75		20000	
m5ad.12xlarge [2]	6780		847,5		30000	
m5ad.16xlarge [2]	9500		1187.5		40000	

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
m5ad.24xlarge [2]	13 750		1718,75		60 000	
m5d.large [1]	650	4750	81,25	593,75	3600	18 750
m5d.xlarge [1]	1150	4750	143,75	593,75	6000	18 750
m5d.2xlarge [1]	2300	4750	287,50	593,75	12 000	18 750
m5d.4xlarge [2]	4750		593,75		18 750	
m5d.8xlarge [2]	6800		850,0		30000	
m5d.12xlarge [2]	9500		1187.5		40000	
m5d.16xlarge [2]	13600		1700,0		60 000	
m5d.24xlarge [2]	19 000		2375,0		80 000	
m5d.metal [2]	19 000		2375,0		80 000	
m5dn.large [1]	650	4750	81,25	593,75	3600	18 750

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
m5dn.xlarge [1]	1150	4750	143,75	593,75	6000	18 750
m5dn.2xlarge [1]	2300	4750	287,50	593,75	12 000	18 750
m5dn.4xlarge [2]	4750		593,75		18 750	
m5dn.8xlarge [2]	6800		850,0		30000	
m5dn.12xlarge [2]	9500		1187.5		40000	
m5dn.16xlarge [2]	13600		1700,0		60 000	
m5dn.24xlarge [2]	19 000		2375,0		80 000	
m5dn.metal [2]	19 000		2375,0		80 000	
m5n.large [1]	650	4750	81,25	593,75	3600	18 750
m5n.xlarge [1]	1150	4750	143,75	593,75	6000	18 750
m5n.2xlarge [1]	2300	4750	287,50	593,75	12 000	18 750

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
m5n.4xlarge [2]	4750		593,75		18 750	
m5n.8xlarge [2]	6800		850,0		30000	
m5n.12xlarge [2]	9500		1187.5		40000	
m5n.16xlarge [2]	13600		1700,0		60 000	
m5n.24xlarge [2]	19 000		2375,0		80 000	
m5n.metal [2]	19 000		2375,0		80 000	
m5zn.large [1]	800	3170	100,00	396,25	3333	13 333
m5zn.xlarge [1]	1564	3170	195,50	396,25	6667	13 333
m5zn.2xlarge [2]	3170		396,25		13 333	
m5zn.3xlarge [2]	4750		593,75		20000	
m5zn.6xlarge [2]	9500		1187.5		40000	

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
m5zn.12xlarge [2]	19 000		2375,0		80 000	
m5zn.metal [2]	19 000		2375,0		80 000	
m6a.large [1]	650	10000	81,25	1250,00	3600	40000
m6a.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
m6a.2xlarge [1]	2 500	10000	312,50	1250,00	12 000	40000
m6a.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
m6a.8xlarge [2]	10000		1250,0		40000	
m6a.12xlarge [2]	15000		1875,0		60 000	
m6a.16xlarge [2]	20000		2500,0		80 000	
m6a.24xlarge [2]	30000		3750,0		120 000	
m6a.32xlarge [2]	40000		5000,0		160 000	

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
m6a.48xlarge [2]	40000		5000,0		240 000	
m6a.metal [2]	40000		5000,0		240 000	
m6g.medium [1]	315	4750	39,38	593,75	2 500	20000
m6g.large [1]	630	4750	78,75	593,75	3600	20000
m6g.xlarge [1]	1188	4750	148,50	593,75	6000	20000
m6g.2xlarge [1]	2375	4750	296,88	593,75	12 000	20000
m6g.4xlarge [2]	4750		593,75		20000	
m6g.8xlarge [2]	9500		1187.5		40000	
m6g.12xlarge [2]	14 250		1781,25		50000	
m6g.16xlarge [2]	19 000		2375,0		80 000	
m6g.metal [2]	19 000		2375,0		80 000	

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
m6gd.medium [1]	315	4750	39,38	593,75	2 500	20000
m6gd.large [1]	630	4750	78,75	593,75	3600	20000
m6gd.xlarge [1]	1188	4750	148,50	593,75	6000	20000
m6gd.2xlarge [1]	2375	4750	296,88	593,75	12 000	20000
m6gd.4xlarge [2]	4750		593,75		20000	
m6gd.8xlarge [2]	9500		1187.5		40000	
m6gd.12xlarge [2]	14 250		1781,25		50000	
m6gd.16xlarge [2]	19 000		2375,0		80 000	
m6gd.metal [2]	19 000		2375,0		80 000	
m6i.large [1]	650	10000	81,25	1250,00	3600	40000
m6i.xlarge [1]	1250	10000	156,25	1250,00	6000	40000

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
m6i.2xlarge [1]	2 500	10000	312,50	1250,00	12 000	40000
m6i.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
m6i.8xlarge [2]	10000		1250,0		40000	
m6i.12xlarge [2]	15000		1875,0		60 000	
m6i.16xlarge [2]	20000		2500,0		80 000	
m6i.24xlarge [2]	30000		3750,0		120 000	
m6i.32xlarge [2]	40000		5000,0		160 000	
m6i.metal [2]	40000		5000,0		160 000	
m6id.large [1]	650	10000	81,25	1250,00	3600	40000
m6id.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
m6id.2xlarge [1]	2 500	10000	312,50	1250,00	12 000	40000

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
m6id.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
m6id.8xlarge [2]	10000		1250,0		40000	
m6id.12xlarge [2]	15000		1875,0		60 000	
m6id.16xlarge [2]	20000		2500,0		80 000	
m6id.24xlarge [2]	30000		3750,0		120 000	
m6id.32xlarge [2]	40000		5000,0		160 000	
m6id.metal [2]	40000		5000,0		160 000	
m6idn.large [1]	1562	25000	195,31	3125,00	6250	100000
m6idn.xlarge [1]	3125	25000	390,62	3125,00	12500	100000
m6idn.2xlarge [1]	6250	25000	781,25	3125,00	25000	100000
m6idn.4xlarge [1]	12500	25000	1562,50	3125,00	50000	100000

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
m6idn.8xlarge [2]	25000		3125,0		100000	
m6idn.12xlarge [2]	37 500		4687,5		150 000	
m6idn.16xlarge [2]	50000		6250,0		200 000	
m6idn.24xlarge [2]	75 000		9375,0		300 000	
m6idn.32xlarge [2]	100000		12 500,0		400 000	
m6idn.metal [2]	100000		12 500,0		400 000	
m6in.large [1]	1562	25000	195,31	3125,00	6250	100000
m6in.xlarge [1]	3125	25000	390,62	3125,00	12500	100000
m6in.2xlarge [1]	6250	25000	781,25	3125,00	25000	100000
m6in.4xlarge [1]	12500	25000	1562,50	3125,00	50000	100000
m6in.8xlarge [2]	25000		3125,0		100000	

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
m6in.12xlarge [2]	37 500		4687,5		150 000	
m6in.16xlarge [2]	50000		6250,0		200 000	
m6in.24xlarge [2]	75 000		9375,0		300 000	
m6in.32xlarge [2]	100000		12 500,0		400 000	
m6in.metal [2]	100000		12 500,0		400 000	
m7a.medium [1]	325	10000	40,62	1250,00	2 500	40000
m7a.large [1]	650	10000	81,25	1250,00	3600	40000
m7a.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
m7a.2xlarge [1]	2 500	10000	312,50	1250,00	12 000	40000
m7a.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
m7a.8xlarge [2]	10000		1250,0		40000	

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
m7a.12xlarge [2]	15000		1875,0		60 000	
m7a.16xlarge [2]	20000		2500,0		80 000	
m7a.24xlarge [2]	30000		3750,0		120 000	
m7a.32xlarge [2]	40000		5000,0		160 000	
m7a.48xlarge [2]	40000		5000,0		240 000	
m7a.metal-48xl [2]	40000		5000,0		240 000	
m7g.medium [1]	315	10000	39,38	1250,00	2 500	40000
m7g.large [1]	630	10000	78,75	1250,00	3600	40000
m7g.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
m7g.2xlarge [1]	2 500	10000	312,50	1250,00	12 000	40000
m7g.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
m7g.8xlarge [2]	10000		1250,0		40000	
m7g.12xlarge [2]	15000		1875,0		60 000	
m7g.16xlarge [2]	20000		2500,0		80 000	
m7g.metal [2]	20000		2500,0		80 000	
m7gd.medium [1]	315	10000	39,38	1250,00	2 500	40000
m7gd.large [1]	630	10000	78,75	1250,00	3600	40000
m7gd.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
m7gd.2xlarge [1]	2 500	10000	312,50	1250,00	12 000	40000
m7gd.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
m7gd.8xlarge [2]	10000		1250,0		40000	
m7gd.12xlarge [2]	15000		1875,0		60 000	

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
m7gd.16xlarge [2]	20000		2500,0		80 000	
m7gd.metal [2]	20000		2500,0		80 000	
m7i.large [1]	650	10000	81,25	1250,00	3600	40000
m7i.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
m7i.2xlarge [1]	2 500	10000	312,50	1250,00	12 000	40000
m7i.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
m7i.8xlarge [2]	10000		1250,0		40000	
m7i.12xlarge [2]	15000		1875,0		60 000	
m7i.16xlarge [2]	20000		2500,0		80 000	
m7i.24xlarge [2]	30000		3750,0		120 000	
m7i.48xlarge [2]	40000		5000,0		240 000	

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
m7i.metal-24xl [2]	30000		3750,0		120 000	
m7i.metal-48xl [2]	40000		5000,0		240 000	
m7i-flex.large [1]	312	10000	39,06	1250,00	2 500	40000
m7i-flex.xlarge [1]	625	10000	78,12	1250,00	3600	40000
m7i-flex.2xlarge [1]	1250	10000	156,25	1250,00	6000	40000
m7i-flex.4xlarge [1]	2 500	10000	312,50	1250,00	12 000	40000
m7i-flex.8xlarge [1]	5000	10000	625,00	1250,00	20000	40000
mac1.metal [2]	14000		1750,0		80 000	
mac2.metal [2]	10000		1250,0		55 000	
mac2-m2.metal [2]	8000		1000,0		55 000	
mac2-m2pro.metal [2]	8000		1000,0		55 000	

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
t3.nano [1]	43	2085	5,38	260,62	250	11 800
t3.micro [1]	87	2085	10,88	260,62	500	11 800
t3.small [1]	174	2085	21,75	260,62	1 000	11 800
t3.medium [1]	347	2085	43,38	260,62	2000	11 800
t3.large [1]	695	2780	86,88	347,50	4000	15 700
t3.xlarge [1]	695	2780	86,88	347,50	4000	15 700
t3.2xlarge [1]	695	2780	86,88	347,50	4000	15 700
t3a.nano [1]	45	2085	5,62	260,62	250	11 800
t3a.micro [1]	90	2085	11,25	260,62	500	11 800
t3a.small [1]	175	2085	21,88	260,62	1 000	11 800
t3a.medium [1]	350	2085	43,75	260,62	2000	11 800
t3a.large [1]	695	2780	86,88	347,50	4000	15 700
t3a.xlarge [1]	695	2780	86,88	347,50	4000	15 700
t3a.2xlarge [1]	695	2780	86,88	347,50	4000	15 700
t4g.nano [1]	43	2085	5,38	260,62	250	11 800
t4g.micro 1	87	2085	10,88	260,62	500	11 800

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
t4g.small [1]	174	2085	21,75	260,62	1 000	11 800
t4g.medium [1]	347	2085	43,38	260,62	2000	11 800
t4g.large 1	695	2780	86,88	347,50	4000	15 700
t4g.xlarge [1]	695	2780	86,88	347,50	4000	15 700
t4g.2xlarge [1]	695	2780	86,88	347,50	4000	15 700

Optimizada para computación

Important

[1] Estas instancias pueden ofrecer el máximo rendimiento durante 30 minutos al menos una vez cada 24 horas, tras lo cual vuelven a su rendimiento básico.

[2] Estas instancias pueden mantener el rendimiento indicado de forma indefinida. Si la carga de trabajo requiere un rendimiento máximo prolongado de más de 30 minutos, utilice una de estas instancias.

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
c4.large [2]	500		62,5		4000	

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
c4.xlarge [2]	750		93,75		6000	
m4.2xlarge [2]	1 000		125,0		8000	
c4.4xlarge [2]	2000		250,0		16 000	
c4.8xlarge [2]	4000		500,0		32 000	
c5.large [1]	650	4750	81,25	593,75	4000	20000
c5.xlarge [1]	1150	4750	143,75	593,75	6000	20000
c5.2xlarge [1]	2300	4750	287,50	593,75	10000	20000
c5.4xlarge [2]	4750		593,75		20000	
c5.9xlarge [2]	9500		1187.5		40000	
c5.12xlarge [2]	9500		1187.5		40000	
c5.18xlarge [2]	19 000		2375,0		80 000	
c5.24xlarge [2]	19 000		2375,0		80 000	
c5.metal [2]	19 000		2375,0		80 000	

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
c5a.large [1]	200	3170	25,00	396,25	800	13 300
c5a.xlarge [1]	400	3170	50,00	396,25	1600	13 300
c5a.2xlarge [1]	800	3170	100,00	396,25	3200	13 300
c5a.4xlarge [1]	1580	3170	197,50	396,25	6600	13 300
c5a.8xlarge [2]	3170		396,25		13 300	
c5a.12xlarge [2]	4750		593,75		20000	
c5a.16xlarge [2]	6300		787,5		26 700	
c5a.24xlarge [2]	9500		1187.5		40000	
c5ad.large [1]	200	3170	25,00	396,25	800	13 300
c5ad.xlarge [1]	400	3170	50,00	396,25	1600	13 300
c5ad.2xlarge [1]	800	3170	100,00	396,25	3200	13 300

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
c5ad.4xlarge [1]	1580	3170	197,50	396,25	6600	13 300
c5ad.8xlarge [2]	3170		396,25		13 300	
c5ad.12xlarge [2]	4750		593,75		20000	
c5ad.16xlarge [2]	6300		787,5		26 700	
c5ad.24xlarge [2]	9500		1187.5		40000	
c5d.large [1]	650	4750	81,25	593,75	4000	20000
c5d.xlarge [1]	1150	4750	143,75	593,75	6000	20000
c5d.2xlarge [1]	2300	4750	287,50	593,75	10000	20000
c5d.4xlarge [2]	4750		593,75		20000	
c5d.9xlarge [2]	9500		1187.5		40000	
c5d.12xlarge [2]	9500		1187.5		40000	

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
c5d.18xlarge [2]	19 000		2375,0		80 000	
c5d.24xlarge [2]	19 000		2375,0		80 000	
c5d.metal [2]	19 000		2375,0		80 000	
c5n.large [1]	650	4750	81,25	593,75	4000	20000
c5n.xlarge [1]	1150	4750	143,75	593,75	6000	20000
c5d.2xlarge [1]	2300	4750	287,50	593,75	10000	20000
c5n.4xlarge [2]	4750		593,75		20000	
c5n.9xlarge [2]	9500		1187.5		40000	
c5n.18xlarge [2]	19 000		2375,0		80 000	
c5n.metal [2]	19 000		2375,0		80 000	
c6a.large [1]	650	10000	81,25	1250,00	3600	40000
c6a.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
c6a.2xlarge [1]	2 500	10000	312,50	1250,00	12 000	40000

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
c6a.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
c6a.8xlarge [2]	10000		1250,0		40000	
c6a.12xlarge [2]	15000		1875,0		60 000	
c6a.16xlarge [2]	20000		2500,0		80 000	
c6a.24xlarge [2]	30000		3750,0		120 000	
c6a.32xlarge [2]	40000		5000,0		160 000	
c6a.48xlarge [2]	40000		5000,0		240 000	
m6a.metal [2]	40000		5000,0		240 000	
c6g.medium [1]	315	4750	39,38	593,75	2 500	20000
c6g.large [1]	630	4750	78,75	593,75	3600	20000
c6g.xlarge [1]	1188	4750	148,50	593,75	6000	20000

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
c6g.2xlarge [1]	2375	4750	296,88	593,75	12 000	20000
c6g.4xlarge [2]	4750		593,75		20000	
c6g.8xlarge [2]	9500		1187.5		40000	
c6g.12xlarge [2]	14 250		1781,25		50000	
c6g.16xlarge [2]	19 000		2375,0		80 000	
c6g.metal [2]	19 000		2375,0		80 000	
c6gd.medium [1]	315	4750	39,38	593,75	2 500	20000
c6gd.large [1]	630	4750	78,75	593,75	3600	20000
c6gd.xlarge [1]	1188	4750	148,50	593,75	6000	20000
c6gd.2xlarge [1]	2375	4750	296,88	593,75	12 000	20000
c6gd.4xlarge [2]	4750		593,75		20000	

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
c6gd.8xlarge [2]	9500		1187.5		40000	
c6gd.12xlarge [2]	14 250		1781,25		50000	
c6gd.16xlarge [2]	19 000		2375,0		80 000	
c6gd.metal [2]	19 000		2375,0		80 000	
c6gn.medium [1]	760	9500	95,00	1187,50	2 500	40000
c6gn.large [1]	1235	9500	154,38	1187,50	5000	40000
c6gn.xlarge [1]	2375	9500	296,88	1187,50	10000	40000
c6gn.2xlarge [1]	4750	9500	593,75	1187,50	20000	40000
c6gn.4xlarge [2]	9500		1187.5		40000	
c6gn.8xlarge [2]	19 000		2375,0		80 000	
c6gn.12xlarge [2]	28 500		3562,5		120 000	

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
c6gn.16xlarge [2]	38 000		4750,0		160 000	
c6i.large [1]	650	10000	81,25	1250,00	3600	40000
c6i.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
c6g.2xlarge [1]	2 500	10000	312,50	1250,00	12 000	40000
c6i.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
c6i.8xlarge [2]	10000		1250,0		40000	
c6i.12xlarge [2]	15000		1875,0		60 000	
c6i.16xlarge [2]	20000		2500,0		80 000	
c6i.24xlarge [2]	30000		3750,0		120 000	
c6i.32xlarge [2]	40000		5000,0		160 000	
c6g.metal [2]	40000		5000,0		160 000	
c6id.large [1]	650	10000	81,25	1250,00	3600	40000
c6id.xlarge [1]	1250	10000	156,25	1250,00	6000	40000

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
c6id.2xlarge [1]	2 500	10000	312,50	1250,00	12 000	40000
c6id.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
c6id.8xlarge [2]	10000		1250,0		40000	
c6id.12xlarge [2]	15000		1875,0		60 000	
c6id.16xlarge [2]	20000		2500,0		80 000	
c6id.24xlarge [2]	30000		3750,0		120 000	
c6id.32xlarge [2]	40000		5000,0		160 000	
c6id.metal [2]	40000		5000,0		160 000	
c6in.large [1]	1562	25000	195,31	3125,00	6250	100000
c6in.xlarge [1]	3125	25000	390,62	3125,00	12500	100000
c6in.2xlarge [1]	6250	25000	781,25	3125,00	25000	100000

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
c6in.4xlarge [1]	12500	25000	1562,50	3125,00	50000	100000
c6in.8xlarge [2]	25000		3125,0		100000	
c6in.12xlarge [2]	37 500		4687,5		150 000	
c6in.16xlarge [2]	50000		6250,0		200 000	
c6in.24xlarge [2]	75 000		9375,0		300 000	
c6in.32xlarge [2]	100000		12 500,0		400 000	
c6in.metal [2]	100000		12 500,0		400 000	
c7a.medium [1]	325	10000	40,62	1250,00	2 500	40000
c7g.large [1]	650	10000	81,25	1250,00	3600	40000
c7a.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
c7a.2xlarge [1]	2 500	10000	312,50	1250,00	12 000	40000

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
c7a.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
c7a.8xlarge [2]	10000		1250,0		40000	
c7a.12xlarge [2]	15000		1875,0		60 000	
c7a.16xlarge [2]	20000		2500,0		80 000	
c7a.24xlarge [2]	30000		3750,0		120 000	
c7a.32xlarge [2]	40000		5000,0		160 000	
c7a.48xlarge [2]	40000		5000,0		240 000	
c7a.metal-48xl [2]	40000		5000,0		240 000	
c7g.medium [1]	315	10000	39,38	1250,00	2 500	40000
c7g.large [1]	630	10000	78,75	1250,00	3600	40000
c7g.xlarge [1]	1250	10000	156,25	1250,00	6000	40000

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
c7g.2xlarge [1]	2 500	10000	312,50	1250,00	12 000	40000
c7g.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
c7g.8xlarge [2]	10000		1250,0		40000	
c7g.12xlarge [2]	15000		1875,0		60 000	
c7g.16xlarge [2]	20000		2500,0		80 000	
c7g.metal [2]	20000		2500,0		80 000	
c7gd.medium [1]	315	10000	39,38	1250,00	2 500	40000
c7gd.large [1]	630	10000	78,75	1250,00	3600	40000
c7gd.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
c7gd.2xlarge [1]	2 500	10000	312,50	1250,00	12 000	40000
c7gd.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
c7gd.8xlarge [2]	10000		1250,0		40000	
c7gd.12xlarge [2]	15000		1875,0		60 000	
c7gd.16xlarge [2]	20000		2500,0		80 000	
c7gd.metal [2]	20000		2500,0		80 000	
c7gn.medium [1]	521	10000	65,12	1250,00	2083	40000
c7gn.large [1]	1042	10000	130,25	1250,00	4167	40000
c7gn.xlarge [1]	2083	10000	260,38	1250,00	8333	40000
c7gn.2xlarge [1]	4167	10000	520,88	1250,00	16 667	40000
c7gn.4xlarge [1]	8333	10000	1041,62	1250,00	33 333	40000
c7gn.8xlarge [1]	16 667	20000	2083,38	2500,00	66 667	80 000
c7gn.12xlarge [1]	25000	30000	3125,00	3750,00	100000	120 000

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
c7gn.16xlarge [1]	33 333	40000	4166,62	5000,00	133 333	160 000
c7gn.metal [1]	33 333	40000	4166,62	5000,00	133 333	160 000
c7i.large [1]	650	10000	81,25	1250,00	3600	40000
c7i.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
c7i.2xlarge [1]	2 500	10000	312,50	1250,00	12 000	40000
c7i.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
c7i.8xlarge [2]	10000		1250,0		40000	
c7i.12xlarge [2]	15000		1875,0		60 000	
c7i.16xlarge [2]	20000		2500,0		80 000	
c7i.24xlarge [2]	30000		3750,0		120 000	
c7i.48xlarge [2]	40000		5000,0		240 000	
c7i.metal-24xl [2]	30000		3750,0		120 000	

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
c7i.metal -48xl [2]	40000		5000,0		240 000	
c7i-flex. large [1]	312	10000	39,06	1250,00	2 500	40000
c7i-flex. xlarge [1]	625	10000	78,12	1250,00	3600	40000
c7i-flex. 2xlarge [1]	1250	10000	156,25	1250,00	6000	40000
c7i-flex. 4xlarge [1]	2 500	10000	312,50	1250,00	12 000	40000
c7i-flex. 8xlarge [1]	5000	10000	625,00	1250,00	20000	40000

Optimizada para memoria

Important

[1] Estas instancias pueden ofrecer el máximo rendimiento durante 30 minutos al menos una vez cada 24 horas, tras lo cual vuelven a su rendimiento básico.

[2] Estas instancias pueden mantener el rendimiento indicado de forma indefinida. Si la carga de trabajo requiere un rendimiento máximo prolongado de más de 30 minutos, utilice una de estas instancias.

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
r4.large [2]	425		53 125		3 000	
r4.xlarge [2]	850		106,25		6000	
r4.2xlarge [2]	1700		212,5		12 000	
r4.4xlarge [2]	3500		437,5		18 750	
r4.8xlarge [2]	7000		875,0		37 500	
r4.16xlarge [2]	14000		1750,0		75 000	
r5.large [1]	650	4750	81,25	593,75	3600	18 750
r5.xlarge [1]	1150	4750	143,75	593,75	6000	18 750
r5.2xlarge [1]	2300	4750	287,50	593,75	12 000	18 750
r5.4xlarge [2]	4750		593,75		18 750	
r5.8xlarge [2]	6800		850,0		30000	
r5.12xlarge [2]	9500		1187.5		40000	

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
r5.16xlarge [2]	13600		1700,0		60 000	
r5.24xlarge [2]	19 000		2375,0		80 000	
r5.metal [2]	19 000		2375,0		80 000	
r5a.large [1]	650	2 880	81,25	360,00	3600	16 000
r5a.xlarge [1]	1085	2 880	135,62	360,00	6000	16 000
r5a.2xlarge [1]	1580	2 880	197,50	360,00	8333	16 000
r5a.4xlarge [2]	2 880		360,0		16 000	
r5a.8xlarge [2]	4750		593,75		20000	
r5a.12xlarge [2]	6780		847,5		30000	
r5a.16xlarge [2]	9500		1187.5		40000	
r5a.24xlarge [2]	13 570		1696,25		60 000	
r5ad.large [1]	650	2 880	81,25	360,00	3600	16 000

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
r5ad.xlarge [1]	1085	2 880	135,62	360,00	6000	16 000
r5ad.2xlarge [1]	1580	2 880	197,50	360,00	8333	16 000
r5ad.4xlarge [2]	2 880		360,0		16 000	
r5ad.8xlarge [2]	4750		593,75		20000	
r5ad.12xlarge [2]	6780		847,5		30000	
r5ad.16xlarge [2]	9500		1187.5		40000	
r5ad.24xlarge [2]	13 570		1696,25		60 000	
r5b.large [1]	1250	10000	156,25	1250,00	5417	43 333
r5b.xlarge [1]	2 500	10000	312,50	1250,00	10 833	43 333
r5b.2xlarge [1]	5000	10000	625,00	1250,00	21 667	43 333
r5b.4xlarge [2]	10000		1250,0		43 333	

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
r5b.8xlarge [2]	20000		2500,0		86 667	
r5b.12xlarge [2]	30000		3750,0		130 000	
r5b.16xlarge [2]	40000		5000,0		173 333	
r5b.24xlarge [2]	60 000		7500,0		260 000	
r5b.metal [2]	60 000		7500,0		260 000	
r5d.large [1]	650	4750	81,25	593,75	3600	18 750
r5d.xlarge [1]	1150	4750	143,75	593,75	6000	18 750
r5d.2xlarge [1]	2300	4750	287,50	593,75	12 000	18 750
r5d.4xlarge [2]	4750		593,75		18 750	
r5d.8xlarge [2]	6800		850,0		30000	
r5d.12xlarge [2]	9500		1187.5		40000	
r5d.16xlarge [2]	13600		1700,0		60 000	

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
r5d.24xlarge [2]	19 000		2375,0		80 000	
r5d.metal [2]	19 000		2375,0		80 000	
r5dn.large [1]	650	4750	81,25	593,75	3600	18 750
r5dn.xlarge [1]	1150	4750	143,75	593,75	6000	18 750
r5dn.2xlarge [1]	2300	4750	287,50	593,75	12 000	18 750
r5dn.4xlarge [2]	4750		593,75		18 750	
r5dn.8xlarge [2]	6800		850,0		30000	
r5dn.12xlarge [2]	9500		1187.5		40000	
r5dn.16xlarge [2]	13600		1700,0		60 000	
r5dn.24xlarge [2]	19 000		2375,0		80 000	
r5dn.metal [2]	19 000		2375,0		80 000	
r5n.large [1]	650	4750	81,25	593,75	3600	18 750

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
r5n.xlarge [1]	1150	4750	143,75	593,75	6000	18 750
r5n.2xlarge [1]	2300	4750	287,50	593,75	12 000	18 750
r5n.4xlarge [2]	4750		593,75		18 750	
r5n.8xlarge [2]	6800		850,0		30000	
r5n.12xlarge [2]	9500		1187.5		40000	
r5n.16xlarge [2]	13600		1700,0		60 000	
r5n.24xlarge [2]	19 000		2375,0		80 000	
r5n.metal [2]	19 000		2375,0		80 000	
r6a.large [1]	650	10000	81,25	1250,00	3600	40000
r6a.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
r6a.2xlarge [1]	2 500	10000	312,50	1250,00	12 000	40000
r6a.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
r6a.8xlarge [2]	10000		1250,0		40000	
r6a.12xlarge [2]	15000		1875,0		60 000	
r6a.16xlarge [2]	20000		2500,0		80 000	
r6a.24xlarge [2]	30000		3750,0		120 000	
r6a.32xlarge [2]	40000		5000,0		160 000	
r6a.48xlarge [2]	40000		5000,0		240 000	
r6a.metal [2]	40000		5000,0		240 000	
r6g.medium [1]	315	4750	39,38	593,75	2 500	20000
r6g.large [1]	630	4750	78,75	593,75	3600	20000
r6g.xlarge [1]	1188	4750	148,50	593,75	6000	20000
r6g.2xlarge [1]	2375	4750	296,88	593,75	12 000	20000
r6g.4xlarge [2]	4750		593,75		20000	

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
r6g.8xlarge [2]	9500		1187.5		40000	
r6g.12xlarge [2]	14 250		1781,25		50000	
r6g.16xlarge [2]	19 000		2375,0		80 000	
r6g.metal [2]	19 000		2375,0		80 000	
r6gd.medium [1]	315	4750	39,38	593,75	2 500	20000
r6gd.large [1]	630	4750	78,75	593,75	3600	20000
r6gd.xlarge [1]	1188	4750	148,50	593,75	6000	20000
r6gd.2xlarge [1]	2375	4750	296,88	593,75	12 000	20000
r6gd.4xlarge [2]	4750		593,75		20000	
r6gd.8xlarge [2]	9500		1187.5		40000	
r6gd.12xlarge [2]	14 250		1781,25		50000	

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
r6gd.16xlarge [2]	19 000		2375,0		80 000	
r6gd.metal [2]	19 000		2375,0		80 000	
r6i.large [1]	650	10000	81,25	1250,00	3600	40000
r6i.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
r6i.2xlarge [1]	2 500	10000	312,50	1250,00	12 000	40000
r6i.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
r6i.8xlarge [2]	10000		1250,0		40000	
r6i.12xlarge [2]	15000		1875,0		60 000	
r6i.16xlarge [2]	20000		2500,0		80 000	
r6i.24xlarge [2]	30000		3750,0		120 000	
r6i.32xlarge [2]	40000		5000,0		160 000	
r6i.metal [2]	40000		5000,0		160 000	

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
r6idn.large [1]	1562	25000	195,31	3125,00	6250	100000
r6idn.xlarge [1]	3125	25000	390,62	3125,00	12500	100000
r6idn.2xlarge [1]	6250	25000	781,25	3125,00	25000	100000
r6idn.4xlarge [1]	12500	25000	1562,50	3125,00	50000	100000
r6idn.8xlarge [2]	25000		3125,0		100000	
r6idn.12xlarge [2]	37 500		4687,5		150 000	
r6idn.16xlarge [2]	50000		6250,0		200 000	
r6idn.24xlarge [2]	75 000		9375,0		300 000	
r6idn.32xlarge [2]	100000		12 500,0		400 000	
r6idn.metal [2]	100000		12 500,0		400 000	
r6in.large [1]	1562	25000	195,31	3125,00	6250	100000

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
r6in.xlarge [1]	3125	25000	390,62	3125,00	12500	100000
r6in.2xlarge [1]	6250	25000	781,25	3125,00	25000	100000
r6in.4xlarge [1]	12500	25000	1562,50	3125,00	50000	100000
r6in.8xlarge [2]	25000		3125,0		100000	
r6in.12xlarge [2]	37 500		4687,5		150 000	
r6in.16xlarge [2]	50000		6250,0		200 000	
r6in.24xlarge [2]	75 000		9375,0		300 000	
r6in.32xlarge [2]	100000		12 500,0		400 000	
r6in.metal [2]	100000		12 500,0		400 000	
r6id.large [1]	650	10000	81,25	1250,00	3600	40000
r6id.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
r6id.2xlarge [1]	2 500	10000	312,50	1250,00	12 000	40000

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
r6id.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
r6id.8xlarge [2]	10000		1250,0		40000	
r6id.12xlarge [2]	15000		1875,0		60 000	
r6id.16xlarge [2]	20000		2500,0		80 000	
r6id.24xlarge [2]	30000		3750,0		120 000	
r6id.32xlarge [2]	40000		5000,0		160 000	
r6id.metal [2]	40000		5000,0		160 000	
r7a.medium [1]	325	10000	40,62	1250,00	2 500	40000
r7a.large [1]	650	10000	81,25	1250,00	3600	40000
r7a.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
r7a.2xlarge [1]	2 500	10000	312,50	1250,00	12 000	40000
r7a.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
r7a.8xlarge [2]	10000		1250,0		40000	
r7a.12xlarge [2]	15000		1875,0		60 000	
r7a.16xlarge [2]	20000		2500,0		80 000	
r7a.24xlarge [2]	30000		3750,0		120 000	
r7a.32xlarge [2]	40000		5000,0		160 000	
r7a.48xlarge [2]	40000		5000,0		240 000	
r7a.metal-48xl [2]	40000		5000,0		240 000	
r7g.medium [1]	315	10000	39,38	1250,00	2 500	40000
r7g.large [1]	630	10000	78,75	1250,00	3600	40000
r7g.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
r7g.2xlarge [1]	2 500	10000	312,50	1250,00	12 000	40000

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
r7g.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
r7g.8xlarge [2]	10000		1250,0		40000	
r7g.12xlarge [2]	15000		1875,0		60 000	
r7g.16xlarge [2]	20000		2500,0		80 000	
r7g.metal [2]	20000		2500,0		80 000	
r7gd.medium [1]	315	10000	39,38	1250,00	2 500	40000
r7gd.large [1]	630	10000	78,75	1250,00	3600	40000
r7gd.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
r7gd.2xlarge [1]	2 500	10000	312,50	1250,00	12 000	40000
r7gd.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
r7gd.8xlarge [2]	10000		1250,0		40000	

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
r7gd.12xlarge [2]	15000		1875,0		60 000	
r7gd.16xlarge [2]	20000		2500,0		80 000	
r7gd.metal [2]	20000		2500,0		80 000	
r7i.large [1]	650	10000	81,25	1250,00	3600	40000
r7i.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
r7i.2xlarge [1]	2 500	10000	312,50	1250,00	12 000	40000
r7i.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
r7i.8xlarge [2]	10000		1250,0		40000	
r7i.12xlarge [2]	15000		1875,0		60 000	
r7i.16xlarge [2]	20000		2500,0		80 000	
r7i.24xlarge [2]	30000		3750,0		120 000	
r7i.48xlarge [2]	40000		5000,0		240 000	

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
r7i.metal-24xl [2]	30000		3750,0		120 000	
r7i.metal-48xl [2]	40000		5000,0		240 000	
r7iz.large [1]	792	10000	99,00	1250,00	3600	40000
r7iz.xlarge [1]	1584	10000	198,00	1250,00	6667	40000
r7iz.2xlarge [1]	3168	10000	396,00	1250,00	13 333	40000
r7iz.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
r7iz.8xlarge [2]	10000		1250,0		40000	
r7iz.12xlarge [2]	19 000		2375,0		76 000	
r7iz.16xlarge [2]	20000		2500,0		80 000	
r7iz.32xlarge [2]	40000		5000,0		160 000	
r7iz.metal-16xl [2]	20000		2500,0		80 000	

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
r7iz.metal-32xl [2]	40000		5000,0		160 000	
u-3tb1.56xlarge [2]	19 000		2375,0		80 000	
u-6tb1.56xlarge [2]	38 000		4750,0		160 000	
u-6tb1.112xlarge [2]	38 000		4750,0		160 000	
u-6tb1.metal [2]	38 000		4750,0		160 000	
u-9tb1.112xlarge [2]	38 000		4750,0		160 000	
u-9tb1.metal [2]	38 000		4750,0		160 000	
u-12tb1.112xlarge [2]	38 000		4750,0		160 000	
u-12tb1.metal [2]	38 000		4750,0		160 000	
u-18tb1.112xlarge [2]	38 000		4750,0		160 000	
u-18tb1.metal [2]	38 000		4750,0		160 000	

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
u-24tb1.112xlarge [2]	38 000		4750,0		160 000	
u-24tb1.metal [2]	38 000		4750,0		160 000	
u7i-12tb.224xlarge [2]	60 000		7500,0		420 000	
u7in-16tb.224xlarge [2]	100000		12 500,0		420 000	
u7in-24tb.224xlarge [2]	100000		12 500,0		420 000	
u7in-32tb.224xlarge [2]	100000		12 500,0		420 000	
x1.16xlarge [2]	7000		875,0		40000	
x1.32xlarge [2]	14000		1750,0		80 000	
x2gd.medium [1]	315	4750	39,38	593,75	2 500	20000
x2gd.large [1]	630	4750	78,75	593,75	3600	20000

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
x2gd.xlarge [1]	1188	4750	148,50	593,75	6000	20000
x2gd.2xlarge [1]	2375	4750	296,88	593,75	12 000	20000
x2gd.4xlarge [2]	4750		593,75		20000	
x2gd.8xlarge [2]	9500		1187.5		40000	
x2gd.12xlarge [2]	14 250		1781,25		60 000	
x2gd.16xlarge [2]	19 000		2375,0		80 000	
x2gd.metal [2]	19 000		2375,0		80 000	
x2idn.16xlarge [2]	40000		5000,0		173 333	
x2idn.24xlarge [2]	60 000		7500,0		260 000	
x2idn.32xlarge [2]	80 000		10 000,0		260 000	
x2idn.metal [2]	80 000		10 000,0		260 000	

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
x2iedn.xlarge [1]	2 500	20000	312,50	2500,00	8125	65 000
x2iedn.2xlarge [1]	5000	20000	625,00	2500,00	16 250	65 000
x2iedn.4xlarge [1]	10000	20000	1250,00	2500,00	32 500	65 000
x2iedn.8xlarge [2]	20000		2500,0		65 000	
x2iedn.16xlarge [2]	40000		5000,0		130 000	
x2iedn.24xlarge [2]	60 000		7500,0		195 000	
x2iedn.32xlarge [2]	80 000		10 000,0		260 000	
x2iedn.metal [2]	80 000		10 000,0		260 000	
x2iezn.2xlarge [2]	3170		396,25		13 333	
x2iezn.4xlarge [2]	4750		593,75		20000	
x2iezn.6xlarge [2]	9500		1187.5		40000	

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
x2iezn.8xlarge [2]	12 000		1500,0		55 000	
x2iezn.12xlarge [2]	19 000		2375,0		80 000	
x2iezn.metal [2]	19 000		2375,0		80 000	
x1e.xlarge [2]	500		62,5		3700	
x1e.2xlarge [2]	1 000		125,0		7400	
x1e.4xlarge [2]	1750		218,75		10000	
x1e.8xlarge [2]	3500		437,5		20000	
x1e.16xlarge [2]	7000		875,0		40000	
x1e.32xlarge [2]	14000		1750,0		80 000	
z1d.large [1]	800	3170	100,00	396,25	3333	13 333
z1d.xlarge [1]	1580	3170	197,50	396,25	6667	13 333

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
z1d.2xlarge [2]	3170		396,25		13 333	
z1d.3xlarge [2]	4750		593,75		20000	
z1d.6xlarge [2]	9500		1187.5		40000	
z1d.12xlarge [2]	19 000		2375,0		80 000	
z1d.metal [2]	19 000		2375,0		80 000	

Optimizada para almacenamiento

Important

[1] Estas instancias pueden ofrecer el máximo rendimiento durante 30 minutos al menos una vez cada 24 horas, tras lo cual vuelven a su rendimiento básico.

[2] Estas instancias pueden mantener el rendimiento indicado de forma indefinida. Si la carga de trabajo requiere un rendimiento máximo prolongado de más de 30 minutos, utilice una de estas instancias.

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
d2.xlarge [2]	750		93,75		6000	
d2.2xlarge [2]	1 000		125,0		8000	
d2.4xlarge [2]	2000		250,0		16 000	
d2.8xlarge [2]	4000		500,0		32 000	
d3.xlarge [1]	850	2800	106,25	350,00	5000	15000
d3.2xlarge [1]	1700	2800	212,50	350,00	10000	15000
d3.4xlarge [2]	2800		350,0		15000	
d3.8xlarge [2]	5000		625,0		30000	
d3en.xlarge [1]	850	2800	106,25	350,00	5000	15000
d3en.2xlarge [1]	1700	2800	212,50	350,00	10000	15000
d3en.4xlarge [2]	2800		350,0		15000	
d3en.6xlarge [2]	4000		500,0		25000	

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
d3en.8xlarge [2]	5000		625,0		30000	
d3en.12xlarge [2]	7000		875,0		40000	
h1.2xlarge [2]	1750		218,75		12 000	
h1.4xlarge [2]	3500		437,5		20000	
h1.8xlarge [2]	7000		875,0		40000	
h1.16xlarge [2]	14000		1750,0		80 000	
i3.large [2]	425		53 125		3 000	
i3.xlarge [2]	850		106,25		6000	
i3.2xlarge [2]	1700		212,5		12 000	
i3.4xlarge [2]	3500		437,5		16 000	
i3.8xlarge [2]	7000		875,0		32 500	
i3.16xlarge [2]	14000		1750,0		65 000	
i3.metal [2]	19 000		2375,0		80 000	
i3en.large [1]	576	4750	72,10	593,75	3 000	20000

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
i3en.xlarge [1]	1153	4750	144,20	593,75	6000	20000
i3en.2xlarge [1]	2307	4750	288,39	593,75	12 000	20000
i3en.3xlarge [1]	3800	4750	475,00	593,75	15000	20000
i3en.6xlarge [2]	4750		593,75		20000	
i3en.12xlarge [2]	9500		1187.5		40000	
i3en.24xlarge [2]	19 000		2375,0		80 000	
i3en.metal [2]	19 000		2375,0		80 000	
i4g.large [1]	625	10000	78,12	1250,00	2 500	40000
i4g.xlarge [1]	1250	10000	156,25	1250,00	5000	40000
i4g.2xlarge [1]	2 500	10000	312,50	1250,00	10000	40000
i4g.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
i4g.8xlarge [2]	10000		1250,0		40000	

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
i4g.16xlarge [2]	20000		2500,0		80 000	
i4i.large [1]	625	10000	78,12	1250,00	2 500	40000
i4i.xlarge [1]	1250	10000	156,25	1250,00	5000	40000
i4i.2xlarge [1]	2 500	10000	312,50	1250,00	10000	40000
i4i.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
i4i.8xlarge [2]	10000		1250,0		40000	
i4i.12xlarge [2]	15000		1875,0		60 000	
i4i.16xlarge [2]	20000		2500,0		80 000	
i4i.24xlarge [2]	30000		3750,0		120 000	
i4i.32xlarge [2]	40000		5000,0		160 000	
i4i.metal [2]	40000		5000,0		160 000	
im4gn.large [1]	1250	10000	156,25	1250,00	5000	40000

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
im4gn.xlarge [1]	2 500	10000	312,50	1250,00	10000	40000
im4gn.2xlarge [1]	5000	10000	625,00	1250,00	20000	40000
im4gn.4xlarge [2]	10000		1250,0		40000	
im4gn.8xlarge [2]	20000		2500,0		80 000	
im4gn.16xlarge [2]	40000		5000,0		160 000	
is4gen.medium [1]	625	10000	78,12	1250,00	2 500	40000
is4gen.large [1]	1250	10000	156,25	1250,00	5000	40000
is4gen.xlarge [1]	2 500	10000	312,50	1250,00	10000	40000
is4gen.2xlarge [1]	5000	10000	625,00	1250,00	20000	40000
is4gen.4xlarge [2]	10000		1250,0		40000	
is4gen.8xlarge [2]	20000		2500,0		80 000	

Computación acelerada

Important

[1] Estas instancias pueden ofrecer el máximo rendimiento durante 30 minutos al menos una vez cada 24 horas, tras lo cual vuelven a su rendimiento básico.

[2] Estas instancias pueden mantener el rendimiento indicado de forma indefinida. Si la carga de trabajo requiere un rendimiento máximo prolongado de más de 30 minutos, utilice una de estas instancias.

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
dl1.24xlarge [2]	19 000		2375,0		80 000	
dl2q.24xlarge [2]	19 000		2375,0		80 000	
f1.2xlarge [2]	1700		212,5		12 000	
f1.4xlarge [2]	3500		437,5		44 000	
f1.16xlarge [2]	14000		1750,0		75 000	
g3.4xlarge [2]	3500		437,5		20000	
g3.8xlarge [2]	7000		875,0		40000	
g3.16xlarge [2]	14000		1750,0		80 000	

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
g4ad.xlarge [1]	400	3170	50,00	396,25	1700	13 333
g4ad.2xlarge [1]	800	3170	100,00	396,25	3400	13 333
g4ad.4xlarge [1]	1580	3170	197,50	396,25	6700	13 333
g4ad.8xlarge [2]	3170		396,25		13 333	
g4ad.16xlarge [2]	6300		787,5		26 667	
g4dn.xlarge [1]	950	3500	118,75	437,50	3 000	20000
g4dn.2xlarge [1]	1150	3500	143,75	437,50	6000	20000
g4dn.4xlarge [2]	4750		593,75		20000	
g4dn.8xlarge [2]	9500		1187.5		40000	
g4dn.12xlarge [2]	9500		1187.5		40000	
g4dn.16xlarge [2]	9500		1187.5		40000	

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
g4dn.metal [2]	19 000		2375,0		80 000	
g5.xlarge [1]	700	3500	87,50	437,50	3 000	15000
g5.2xlarge [1]	850	3500	106,25	437,50	3500	15000
g5.4xlarge [2]	4750		593,75		20000	
g5.8xlarge [2]	16 000		2000,0		65 000	
g5.12xlarge [2]	16 000		2000,0		65 000	
g5.16xlarge [2]	16 000		2000,0		65 000	
g5.24xlarge [2]	19 000		2375,0		80 000	
g5.48xlarge [2]	19 000		2375,0		80 000	
g5g.xlarge [1]	1188	4750	148,50	593,75	6000	20000
g5g.2xlarge [1]	2375	4750	296,88	593,75	12 000	20000

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
g5g.4xlarge [2]	4750		593,75		20000	
g5g.8xlarge [2]	9500		1187.5		40000	
g5g.16xlarge [2]	19 000		2375,0		80 000	
g5g.metal [2]	19 000		2375,0		80 000	
g6.xlarge [1]	1 000	5000	125,00	625,00	4000	20000
g6.2xlarge [1]	2000	5000	250,00	625,00	8000	20000
g6.4xlarge [2]	8000		1000,0		32 000	
g6.8xlarge [2]	16 000		2000,0		64 000	
g6.12xlarge [2]	20000		2500,0		80 000	
g6.16xlarge [2]	20000		2500,0		80 000	
g6.24xlarge [2]	30000		3750,0		120 000	
g6.48xlarge [2]	60 000		7500,0		240 000	

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
gr6.4xlarge [2]	8000		1000,0		32 000	
gr6.8xlarge [2]	16 000		2000,0		64 000	
inf1.xlarge [1]	1190	4750	148,75	593,75	4000	20000
inf1.2xlarge [1]	1190	4750	148,75	593,75	6000	20000
inf1.6xlarge [2]	4750		593,75		20000	
inf1.24xlarge [2]	19 000		2375,0		80 000	
inf2.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
inf2.8xlarge [2]	10000		1250,0		40000	
inf2.24xlarge [2]	30000		3750,0		120 000	
inf2.48xlarge [2]	60 000		7500,0		240 000	
p2.xlarge [2]	750		93,75		6000	

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
p2.8xlarge [2]	5000		625,0		32 500	
p2.16xlarge [2]	10000		1250,0		65 000	
p3.2xlarge [2]	1750		218,75		10000	
p3.8xlarge [2]	7000		875,0		40000	
p3.16xlarge [2]	14000		1750,0		80 000	
p3dn.24xlarge [2]	19 000		2375,0		80 000	
p4d.24xlarge [2]	19 000		2375,0		80 000	
p4de.24xlarge [2]	19 000		2375,0		80 000	
p5.48xlarge [2]	80 000		10 000,0		260 000	
trn1.2xlarge [1]	5000	20000	625,00	2500,00	16 250	65 000
trn1.32xlarge [2]	80 000		10 000,0		260 000	

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
trn1n.32xlarge [2]	80 000		10 000,0		260 000	
vt1.3xlarge [1]	2375	4750	296,88	593,75	10000	20000
vt1.6xlarge [2]	4750		593,75		20000	
vt1.24xlarge [2]	19 000		2375,0		80 000	

Computación de alto rendimiento

> **Important**
>
> [1] Estas instancias pueden ofrecer el máximo rendimiento durante 30 minutos al menos una vez cada 24 horas, tras lo cual vuelven a su rendimiento básico.
>
> [2] Estas instancias pueden mantener el rendimiento indicado de forma indefinida. Si la carga de trabajo requiere un rendimiento máximo prolongado de más de 30 minutos, utilice una de estas instancias.

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
hpc6a.48xlarge [1]	87	2085	10,88	260,62	500	11 000

Tamaño de instancia	Ancho de banda básico (Mbps)	Ancho de banda máximo (Mbps)	Velocidad básica (MB/s, E/S de 128 KiB)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS básico (E/S de 16 KiB)	IOPS máximas (E/S de 16 KiB)
hpc6id.32xlarge [1]	87	2085	10,88	260,62	500	11 000
hpc7a.12xlarge [1]	87	2085	10,88	260,62	500	11 000
hpc7a.24xlarge [1]	87	2085	10,88	260,62	500	11 000
hpc7a.48xlarge [1]	87	2085	10,88	260,62	500	11 000
hpc7a.96xlarge [1]	87	2085	10,88	260,62	500	11 000
hpc7g.4xlarge [1]	87	2085	10,88	260,62	500	11 000
hpc7g.8xlarge [1]	87	2085	10,88	260,62	500	11 000
hpc7g.16xlarge [1]	87	2085	10,88	260,62	500	11 000

Optimización de EBS admitida

En la tabla siguiente se indican los tipos de instancias que admiten la optimización de EBS, pero sin que esté habilitada de forma predeterminada. Puede habilitar la optimización de EBS al iniciar estas instancias o una vez que se estén ejecutando. Las instancias deben tener habilitada la optimización para EBS para alcanzar el nivel de rendimiento descrito. Cuando habilita la optimización para EBS en una instancia que no está optimizada para EBS de manera predeterminada, paga una pequeña tarifa adicional por hora por la capacidad dedicada. Para obtener información acerca de los precios,

consulte instancias optimizadas para EBS en la página de Precios, precios bajo demanda de Amazon EC2.

> **Note**
>
> También puede ver esta información mediante programación con la AWS CLI. Para obtener más información, consulte Ver los tipos de instancias que admiten la optimización de EBS.

Tamaño de instancia	Ancho de banda máximo (Mbps)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS máximas (E/S de 16 KiB)
c1.xlarge	1 000	125,0	8000
c3.xlarge	500	62,5	4000
c3.2xlarge	1 000	125,0	8000
c3.4xlarge	2000	250,0	16 000
i2.xlarge	500	62,5	4000
i2.2xlarge	1 000	125,0	8000
i2.4xlarge	2000	250,0	16 000
m1.large	500	62,5	4000
m1.xlarge	1 000	125,0	8000
m2.2xlarge	500	62,5	4000
m2.4xlarge	1 000	125,0	8000
m3.xlarge	500	62,5	4000
m3.2xlarge	1 000	125,0	8000
r3.xlarge	500	62,5	4000

Tamaño de instancia	Ancho de banda máximo (Mbps)	Velocidad máxima (MB/s, E/S de 128 KiB)	IOPS máximas (E/S de 16 KiB)
r3.2xlarge	1 000	125,0	8000
r3.4xlarge	2000	250,0	16 000

Las instancias `i2.8xlarge`, `c3.8xlarge` y `r3.8xlarge` no disponen de ancho de banda dedicado para EBS y, por lo tanto, no ofrecen la optimización para EBS. En estas instancias, el tráfico de red y el tráfico de Amazon EBS comparten la misma interfaz de red de 10 gigabits.

Obtener el máximo rendimiento

Puede utilizar las métricas `EBSIOBalance%` y `EBSByteBalance%` para ayudarle a determinar si las instancias tienen el tamaño correcto. Puede ver estas métricas en la consola de CloudWatch y establecer una alarma que se active en función del umbral que especifique. Estas métricas se expresan como un porcentaje. Las instancias que tengan sistemáticamente un porcentaje de equilibrio bajo son candidatas a un aumento de tamaño. Las instancias en las que el porcentaje de equilibrio nunca baje del 100 % son candidatas a una reducción de tamaño. Para obtener más información, consulte Monitorear las instancias con CloudWatch.

Estas instancias de memoria elevada se han diseñado para ejecutar bases de datos en memoria grandes, lo que incluye la implementación de producción de la base de datos en memoria SAP HANA, en la nube. Para maximizar el rendimiento de EBS, utilice instancias de memoria elevada con un número par de volúmenes `io1` o `io2` con un rendimiento provisionado idéntico. Por ejemplo, para cargas de trabajo pesadas de IOPS, utilice cuatro volúmenes `io1` o `io2` con 40 000 IOPS provisionadas para obtener el máximo de 160 000 IOPS de instancia. Del mismo modo, para cargas de trabajo de rendimiento pesado, utilice seis volúmenes `io1` o `io2` con 48 000 IOPS provisionadas para obtener el rendimiento máximo de 4750 MB/s. Para obtener recomendaciones adicionales, consulte Configuración de almacenamiento para SAP HANA.

Consideraciones

- Las instancias G4dn, I3en, Inf1, M5a, M5ad, R5a, R5ad, T3, T3a y Z1d iniciadas después del 26 de febrero de 2020 proporcionan el rendimiento máximo indicado en la tabla anterior. Para obtener el máximo rendimiento de una instancia iniciada antes del 26 de febrero de 2020, deténgala e iníciela.

- Las instancias C5, C5d, C5n, M5, M5d, M5n, M5dn, R5, R5d, R5n, R5dn y P3dn iniciadas después del 3 de diciembre de 2019 proporcionan el rendimiento máximo indicado en la tabla anterior. Para obtener el máximo rendimiento de una instancia iniciada antes del 3 de diciembre de 2019, deténgala e iníciela.
- Las instancias `u-6tb1.metal`, `u-9tb1.metal` y `u-12tb1.metal` iniciadas después del 12 de marzo de 2020 proporcionan el rendimiento en la tabla anterior. Las instancias de estos tipos iniciadas antes del 12 de marzo de 2020 podrían proporcionar un rendimiento inferior. Para obtener el máximo rendimiento de una instancia iniciada antes del 12 de marzo de 2020, póngase en contacto con su equipo de cuenta para actualizar la instancia sin costo adicional.

Ver los tipos de instancias que admiten la optimización de EBS

Puede utilizar la AWS CLI para ver los tipos de instancias que admiten la optimización de EBS en la región actual.

Para ver los tipos de instancias que admiten la optimización de EBS y que la tienen habilitada de forma predeterminada

Utilice el siguiente comando: describe-instance-types. Si ejecuta este comando en un Símbolo del sistema de Windows, sustituya los caracteres de continuación de línea \ por el carácter ^.

```
aws ec2 describe-instance-types \
--query 'InstanceTypes[].{InstanceType:InstanceType,"MaxBandwidth(Mb/
s)":EbsInfo.EbsOptimizedInfo.MaximumBandwidthInMbps,MaxIOPS:EbsInfo.EbsOptimizedInfo.MaximumIop
s)":EbsInfo.EbsOptimizedInfo.MaximumThroughputInMBps}' \
--filters Name=ebs-info.ebs-optimized-support,Values=default --output=table
```

Resultado de ejemplo para `eu-west-1`:

```
-------------------------------------------------------------------------
|                          DescribeInstanceTypes                        |
+------------------+---------------------+-----------+-----------------------+
|   InstanceType   | MaxBandwidth(Mb/s)  |  MaxIOPS  |  MaxThroughput(MB/s)  |
+------------------+---------------------+-----------+-----------------------+
|  m5dn.8xlarge    |  6800               |  30000    |  850.0                |
|  m6gd.xlarge     |  4750               |  20000    |  593.75               |
|  c4.4xlarge      |  2000               |  16000    |  250.0                |
|  r4.16xlarge     |  14000              |  75000    |  1750.0               |
|  m5ad.large      |  2880               |  16000    |  360.0                |
```

```
...
```

Para ver los tipos de instancias que admiten la optimización de EBS pero que no la tienen habilitada de forma predeterminada

Utilice el siguiente comando: describe-instance-types.

```
aws ec2 describe-instance-types \
--query 'InstanceTypes[].{InstanceType:InstanceType,"MaxBandwidth(Mb/
s)":EbsInfo.EbsOptimizedInfo.MaximumBandwidthInMbps,MaxIOPS:EbsInfo.EbsOptimizedInfo.MaximumIop
s)":EbsInfo.EbsOptimizedInfo.MaximumThroughputInMBps}' \
--filters Name=ebs-info.ebs-optimized-support,Values=supported --output=table
```

Resultado de ejemplo para `eu-west-1`:

```
-------------------------------------------------------------------------
|                        DescribeInstanceTypes                          |
+--------------+----------------------+----------+-----------------------+
| InstanceType | MaxBandwidth(Mb/s)   | MaxIOPS  |  MaxThroughput(MB/s)  |
+--------------+----------------------+----------+-----------------------+
|  i2.2xlarge  |  1000                |  8000    |  125.0                |
|  m2.4xlarge  |  1000                |  8000    |  125.0                |
|  m2.2xlarge  |  500                 |  4000    |  62.5                 |
|  c1.xlarge   |  1000                |  8000    |  125.0                |
|  i2.xlarge   |  500                 |  4000    |  62.5                 |
|  m3.xlarge   |  500                 |  4000    |  62.5                 |
|  m1.xlarge   |  1000                |  8000    |  125.0                |
|  r3.4xlarge  |  2000                |  16000   |  250.0                |
|  r3.2xlarge  |  1000                |  8000    |  125.0                |
|  c3.xlarge   |  500                 |  4000    |  62.5                 |
|  m3.2xlarge  |  1000                |  8000    |  125.0                |
|  r3.xlarge   |  500                 |  4000    |  62.5                 |
|  i2.4xlarge  |  2000                |  16000   |  250.0                |
|  c3.4xlarge  |  2000                |  16000   |  250.0                |
|  c3.2xlarge  |  1000                |  8000    |  125.0                |
|  m1.large    |  500                 |  4000    |  62.5                 |
+--------------+----------------------+----------+-----------------------+
```

Habilitar la optimización de EBS en la inicialización

Para habilitar la optimización de una instancia, defina su atributo de optimización de EBS.

Para habilitar la optimización para Amazon EBS cuando se inicia una instancia con la consola

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 imagen de máquina de Amazon (AMI)), seleccione una AMI.
4. In Step 2: Choose an Instance Type (Paso 2: Elegir un tipo de instancia), seleccione un tipo de instancia que admita la optimización para Amazon EBS.
5. En Step 3: Configure Instance Details (Paso 3: Configurar los detalles de la instancia), rellene los campos necesarios y elija Launch as EBS-optimized instance (iniciar como instancia optimizada para EBS). Si el tipo de instancia que ha seleccionado en el paso anterior no admite la optimización para Amazon EBS, esta opción no está presente. Si el tipo de instancia que ha seleccionado está optimizada para Amazon EBS de forma predeterminada, esta opción está seleccionada y no puede anular la selección.
6. Siga las direcciones hasta finalizar el asistente y lance la instancia.

Para habilitar la optimización para EBS cuando se inicia una instancia desde la línea de comandos

Puede usar uno de estos comandos con la opción correspondiente. Para obtener más información acerca de estas interfaces de línea de comandos, consulte Acceder a Amazon EC2.

- run-instances con `--ebs-optimized` (AWS CLI)
- New-EC2Instance con `-EbsOptimized` (AWS Tools for Windows PowerShell)

Habilitar la optimización de EBS de una instancia en existente

Para habilitar o desactivar la optimización de una instancia existente, modifique su atributo de instancia optimizada para Amazon EBS. Si la instancia se está ejecutando, primero debe detenerla.

> **Warning**
>
> Cuando detiene una instancia, se borran los datos contenidos en todos los volúmenes de almacén de instancias. Para conservar los datos de los volúmenes del almacén de instancias, asegúrese de realizar una copia de seguridad de ellos en un almacenamiento persistente.

Para habilitar la optimización para EBS de una instancia existente desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instances (instancia[s]) y seleccione la instancia.
3. Para detener la instancia, elija Actions (Acciones), Instance state (Estado de la instancia) y Stop instance (Detener instancia). Puede que transcurran unos minutos hasta que la instancia se detenga.
4. Con la instancia aún seleccionada, elija Actions (Acciones), Instance settings (Configuración de la instancia), Change instance type (Cambiar tipo de instancia).
5. Para Change Instance Type (Cambiar tipo de instancia), realice una de las acciones siguientes:
   - Si el tipo de la instancia está optimizado para Amazon EBS de forma predeterminada, EBS-optimized (Optimizado para EBS) estará seleccionado y no podrá cambiarlo. Puede elegir Cancel (Cancelar), dado que la optimización para Amazon EBS ya está habilitada para la instancia.
   - Si el tipo de la instancia admite la optimización para Amazon EBS, elija EBS-optimized (Optimizada para EBS) y, a continuación, Apply (Aplicar).
   - Si el tipo de la instancia no admite la optimización para Amazon EBS, no puede elegir EBS-optimized (Optimizada para EBS). Puede seleccionar un tipo de instancia desde Instance Type (Tipo de instancia) que admita la optimización de Amazon EBS y, a continuación, elija EBS-optimized (Optimizada para EBS) y, a continuación, Apply (Aplicar).
6. Elija Instance state (Estado de la instancia) y Start instance (Iniciar instancia).

Para habilitar la optimización para EBS de una instancia existente desde la línea de comandos

1. Si la instancia se está ejecutando, utilice uno de los siguientes comandos para detenerla:
   - stop-instances (AWS CLI)
   - Stop-EC2Instance (AWS Tools for Windows PowerShell)
2. Para habilitar la optimización de EBS, utilice uno de los siguientes comandos con la opción correspondiente:
   - modify-instance-attribute con `--ebs-optimized` (AWS CLI)
   - Edit-EC2InstanceAttribute con `-EbsOptimized` (AWS Tools for Windows PowerShell)

Opciones de compra de instancias

Amazon EC2 proporciona las siguientes opciones de compra para que pueda optimizar los costos en función de sus necesidades:

- instancias bajo demanda: pague, por segundo, solo las instancias que lance.
- Savings Plans: reduzca los costos de Amazon EC2 comprometiéndose a una cantidad de uso constante, en USD por hora, durante un periodo de 1 o 3 años.
- Instancias reservadas: reduzca sus costos de Amazon EC2 comprometiéndose a tener una configuración de instancia coherente, incluido el tipo de instancia y la región, por un periodo de 1 o 3 años.
- instancias de spot: solicite instancias de EC2 no utilizadas, que pueden reducir sus costos de Amazon EC2 considerablemente.
- Dedicated Hosts (Hosts dedicados): pague por un host físico dedicado exclusivamente a ejecutar sus instancias y utilice sus propias licencias de software por socket, por núcleo o por VM para reducir costos.
- instancias dedicadas: pague por hora las instancias que se ejecutan en hardware de usuario único.
- Reservas de capacidad: reserva de capacidad para las instancias de EC2 en una zona de disponibilidad específica.

Si no puede comprometerse con una configuración de instancia específica, pero sí puede comprometerse con una cantidad de uso, compre Savings Plans para reducir los costos de las instancias bajo demanda.Si necesita una reserva de capacidad, compre instancias reservadas o reservas de capacidad para una zona de disponibilidad específica. bloques de capacidad se puede usar para reservar un clúster de instancias de GPU. Las instancias de spot son una opción rentable si es flexible con respecto a cuándo es necesario ejecutar las aplicaciones y si las aplicaciones se pueden interrumpir. Los hosts dedicados o las instancias dedicadas pueden ayudarlo a cumplir los requisitos de conformidad y reducir los costos mediante las licencias de software existentes vinculadas al servidor. Para obtener más información, consulte Precios de Amazon EC2.

Para obtener más información sobre Savings Plans, consulte la Guía del usuario de Savings Plans.

Contenido

- Reserved Instances
- Spot Instances
- Dedicated Hosts
- Dedicated Instances
- Reservas de capacidad

Determinar el ciclo de vida de una instancia

El ciclo de vida de una instancia comienza cuando se inicia y finaliza cuando se termina. La opción de compra que se elige afecta al ciclo de vida de la instancia. Por ejemplo, una instancia a petición se ejecuta cuando se inicia y finaliza cuando se termina. Una instancia de spot se ejecuta mientras haya capacidad disponible y el precio máximo sea superior al precio de spot.

Utilice uno de los métodos siguientes para determinar el ciclo de vida de una instancia.

Para determinar el ciclo de vida de la instancia con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instancias.
3. Seleccione la instancia.
4. En la pestaña Details (Detalles) en Instance details (Detalles de instancia), busque Lifecycle (Ciclo de vida). Si el valor es `spot`, la instancia es una instancia de spot. Si el valor es `normal`, la instancia es una instancia a petición o una instancia reservada.
5. En la pestaña Details (Detalles), en Host and placement group (Host y grupo de ubicación), busque Tenancy (Tenencia). Si el valor es `host`, la instancia se ejecuta en un host dedicado. Si el valor es `dedicated`, la instancia es una instancia dedicada.

Para determinar el ciclo de vida de la instancia con la AWS CLI

Utilice el siguiente comando describe-instances:

```
aws ec2 describe-instances --instance-ids i-1234567890abcdef0
```

Si la instancia se está ejecutando en un host dedicado, la salida contiene la información siguiente:

```
"Tenancy": "host"
```

Si la instancia es una instancia dedicada, la salida contiene la información siguiente:

```
"Tenancy": "dedicated"
```

Si la instancia es una instancia de spot, la salida contiene la información siguiente:

```
"InstanceLifecycle": "spot"
```

En cualquier otro caso, la salida no contiene `InstanceLifecycle`.

instancias bajo demanda

Con instancias bajo demanda, paga la capacidad informática por segundo, sin compromisos a largo plazo. Tiene control total sobre el ciclo de vida de la instancia, puede decidir cuándo ejecutarla, detenerla, hibernarla, iniciarla, reiniciarla o terminarla.

No se requiere un compromiso a largo plazo al comprar instancias bajo demanda. Solo paga por los segundos que su instancias bajo demanda esté en estado `running`, con un mínimo de 60 segundos. El precio por segundo para una instancia bajo demanda en ejecución es fijo, y se muestra en la página de Precios bajo demanda, precios de Amazon EC2.

Recomendamos que use instancias bajo demanda para aplicaciones con cargas de trabajo irregulares a corto plazo que no pueden interrumpirse.

Para ahorros importantes en instancias bajo demanda, utilice los Savings Plans de AWS, Spot Instances o Reserved Instances.

Contenido

Cuotas de las instancias bajo demanda

Existen cuotas en la cantidad de instancias bajo demanda en ejecución por Cuenta de AWS por región. Hay cuotas para la cantidad de instancias bajo demanda que se administran en términos de la cantidad de unidades de procesamiento central virtuales (CPU virtuales) que sus instancias

bajo demanda en ejecución estén utilizando, sin importar el tipo de instancia. Cada tipo de cuota especifica el número máximo de CPU virtuales para una o más familias de instancias.

Su cuenta incluye las cuotas siguientes para las instancias bajo demanda. Las cuotas se aplican solo a las instancias en ejecución. Si su instancia está pendiente, en parada, detenida o en hibernación, no se tendrá en cuenta para sus cuotas.

Nombre	Valor predeterminado	Ajustable
Ejecución de instancias DL bajo demanda	0	Sí
Ejecución de instancias F bajo demanda	0	Sí
Ejecución de las instancias G y VT bajo demanda	0	Sí
Ejecución de instancias HPC bajo demanda	0	Sí
Ejecución de instancias bajo demanda de memoria elevada	0	Sí
Ejecución de instancias Inf bajo demanda	0	Sí
Ejecución de instancias P bajo demanda	0	Sí
instancias estándar de ejecución bajo demanda (A, C, D, H, I, M, R, T, Z)	5	Sí
Ejecución de instancias Trn bajo demanda	0	Sí
Ejecución de instancias X bajo demanda	0	Sí

Para obtener información acerca de las diferentes familias, generaciones y tamaños de instancias, consulte la Guía de tipos de instancia de Amazon EC2.

Puede iniciar cualquier combinación de tipos de instancias que satisfagan las necesidades cambiantes de su aplicación, siempre y cuando la cantidad de CPU virtuales no supere la cuota de la cuenta. Por ejemplo, con una cuota de instancias estándar de 256 CPU virtuales, puede iniciar 32 instancias `m5.2xlarge` (CPU virtuales de 32 x 8) o 16 instancias `c5.4xlarge` (CPU virtuales de 16 x 16). Para obtener más información, consulte Límites instancia bajo demanda de EC2.

Tareas

- Monitoreo de las cuotas y uso de las instancias bajo demanda
- Solicitud de un aumento de cuota.

Monitoreo de las cuotas y uso de las instancias bajo demanda

Puede ver y administrar las cuotas de sus instancias bajo demanda utilizando los métodos siguientes.

Visualización de las cuotas actuales desde la consola de Service Quotas

1. Abra la consola de Service Quotas en https://console.aws.amazon.com/servicequotas/home/services/ec2/quotas/.
2. En la barra de navegación, seleccione una región.
3. En el campo de filtro, ingrese **`On-Demand`**.
4. La columna Valor de cuota aplicado muestra la cantidad máxima de CPU virtuales para cada tipo de cuota de instancia bajo demanda para su cuenta.

Para ver las cuotas actuales desde la consola de AWS Trusted Advisor

Abra la página Límites de servicio de la consola de AWS Trusted Advisor.

Para configurar alarmas de CloudWatch

Con la integración de métricas de Amazon CloudWatch, puede monitorear el uso de EC2 según sus cuotas. También puede configurar alarmas para recibir advertencias cuando se acerque a las cuotas. Para obtener más información, consulte Service Quotas y alarmas de Amazon CloudWatch en la Guía del usuario de Service Quotas.

Solicitud de un aumento de cuota.

Aunque Amazon EC2 aumenta automáticamente las cuotas de instancias bajo demanda en función del uso, puede solicitar un aumento de la cuota si es necesario. Por ejemplo, si tiene intención de iniciar más instancias de lo que permite su cuota actual, puede solicitar un aumento de la cuota mediante la consola de Service Quotas, tal como se describe en Cuotas de servicio de Amazon EC2.

Consultar los precios de las instancias bajo demanda

Puede utilizar la API del servicio de lista de precios o la API de lista de precios de AWS para consultar los precios de instancias bajo demanda. Para obtener más información, consulte Usar la lista de precios de AWS de la API en la Guía del usuario de AWS Billing.

Reserved Instances

> **Important**
>
> Recomendamos Savings Plans en lugar de instancias reservadas. Los Savings Plans son la forma más fácil y flexible de ahorrar dinero en costos informáticos de AWS y ofrecen precios más bajos (hasta un 72 % de descuento en los precios bajo demanda), al igual que las instancias reservadas. Sin embargo, los Savings Plans son diferentes a las instancias reservadas. Con instancias reservadas, usted se compromete a una configuración de instancia específica; por otro lado, con Savings Plans, tiene la flexibilidad para usar las configuraciones de instancia que mejor satisfagan sus necesidades. Con Savings Plans, se compromete a una cantidad de uso constante, medido en USD por hora. Para obtener más información, consulte la Guía del usuario de Savings Plans de AWS.

Las instancias reservadas ofrecen un ahorro importante para sus costos de Amazon EC2 en comparación con los precios de las instancias bajo demanda. Las instancias reservadas no son instancias físicas, sino más bien un descuento de facturación que se aplica al uso de instancias bajo demanda en su cuenta. Estas instancias bajo demanda deben tener determinados atributos, como el tipo de instancia y la región para poder aprovechar el descuento de facturación.

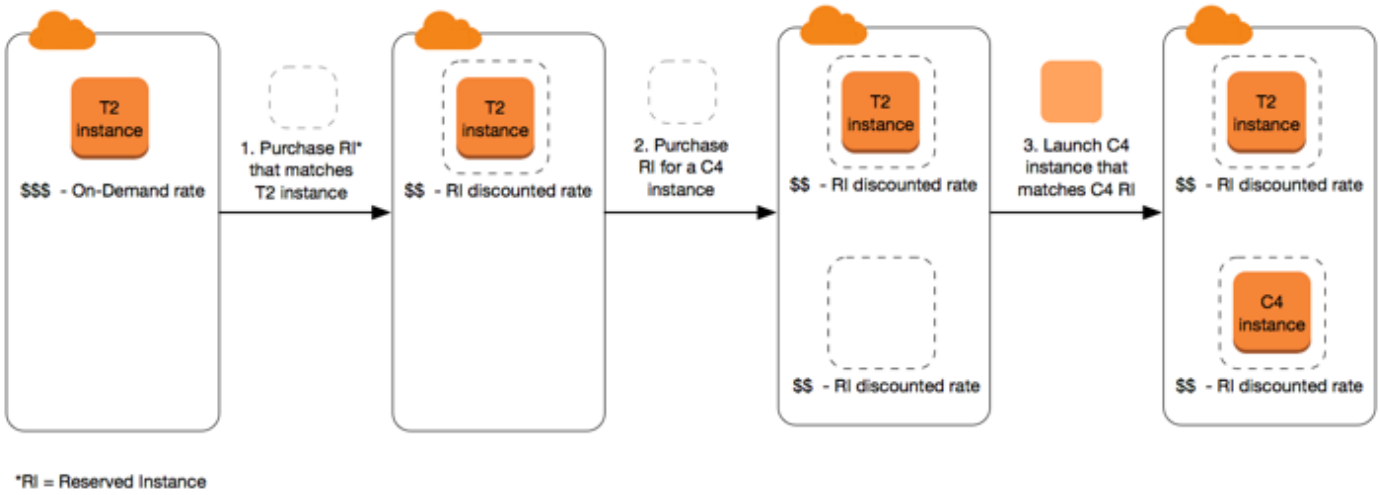
Temas de instancias reservadas

- Información general de instancia reservada
- Variables clave que determinan los precios de instancia reservada
- instancias reservadas regionales y de zona (alcance)
- Tipos de instancias reservadas (clases de oferta)
- Aplicación de las instancias reservadas
- Utilizar su instancias reservadas
- Cómo se le factura

- Comprar instancias reservadas
- Vender en el Marketplace de instancias reservadas
- Modificar instancias reservadas
- Intercambiar instancias reservadas convertibles
- Cuotas de instancia reservada

Información general de instancia reservada

En el siguiente diagrama se muestra información general básica sobre la compra y el uso de instancias reservadas.



En este escenario, tiene una instancia a petición (T2) en ejecución en la cuenta, por la que actualmente está pagando tarifas bajo demanda. Compra una instancia reservada que coincide con los atributos de la instancia en ejecución y el beneficio de facturación se le aplica de forma inmediata. A continuación, compra una instancia reservada para una instancia C4. En la cuenta no tiene ninguna instancia en ejecución que coincida con los atributos de esta instancia reservada. En el paso final, inicia una instancia que coincide con los atributos de la instancia reservada C4 y el beneficio de facturación se le aplica de forma inmediata.

Variables clave que determinan los precios de instancia reservada

El precio de instancia reservada se determina en función de las siguientes variables clave.

Atributos de instancia

Una instancia reservada tiene cuatro atributos de instancia que determinan su precio.

- Tipo de instancia: por ejemplo, `m4.large`. Este atributo se compone de la familia de la instancia (por ejemplo, `m4`) y del tamaño de la instancia (por ejemplo, `large`).
- Región: región en la que se compra instancia reservada.
- Tenencia: indicia si la instancia se ejecuta en hardware compartido (predeterminado) o de un solo propietario (dedicado). Para obtener más información, consulte Dedicated Instances.
- Plataforma: el sistema operativo; por ejemplo, Windows o Linux/Unix. Para obtener más información, consulte Selección de una plataforma.

Compromiso de plazo

Puede comprar una instancia reservada con un compromiso de un año o de tres años, la oferta de compromiso de tres años proporciona un descuento mayor.

- Un año: un año se define como 31 536 000 segundos (365 días).
- Tres años: tres años se definen como 94 608 000 segundos (1095 días).

Las instancias reservadas no se renuevan automáticamente; cuando caducan, usted puede seguir utilizando la instancia de EC2 sin interrupciones, aunque se le cobran las tarifas bajo demanda. En el ejemplo anterior, cuando caducan las instancias reservadas que cubren las instancias T2 y C4, usted vuelve a pagar las tarifas bajo demanda hasta que termine las instancias o compre instancias reservadas nuevas que coincidan con los atributos de instancia.

> **Important**
>
> Una vez que adquiere una instancia reservada, no puede cancelar la compra. Sin embargo, puede modificar, intercambiar o vender la instancia reservada si cambian sus necesidades.

Opciones de pago

Las siguientes opciones de pago están disponibles para las instancias reservadas:

- Pago inicial total: se realiza un pago total al principio del plazo y no se aplicará ningún otro costo ni cargo por hora adicional el resto del plazo, independientemente de las horas de uso.
- Pago inicial parcial: una parte del costo se debe pagar de forma anticipada, y las demás horas del plazo se facturan con una tarifa por horas con descuento, independientemente de si se usa la instancia reservada o no.

- Sin pago inicial: se le cobra una tarifa por hora con descuento por cada hora dentro del plazo, independientemente de si usa la instancia reservada o no. No se requiere ningún pago inicial.

> **Note**
>
> Ninguna instancia de instancias reservadas sin gastos iniciales se basa en una obligación contractual de pagar mensualmente por el plazo completo de la reserva. Por este motivo, se requiere tener un historial de facturación exitoso para poder comprar instancias reservadas sin gastos iniciales.

En términos generales, puede ahorrar más dinero si elige un pago inicial más elevado para instancias reservadas. También puede encontrar instancias reservadas ofrecidas por vendedores externos a precios más bajos y plazos más cortos en el Marketplace de instancias reservadas. Para obtener más información, consulte Vender en el Marketplace de instancias reservadas.

Clase de oferta

Si sus necesidades computacionales cambian, puede modificar o intercambiar la instancia reservada según la clase de oferta.

- Estándar: ofrecen el descuento más importante, pero solo se pueden modificar. Estándar instancias reservadas no se puede intercambiar.
- Convertible: ofrecen un descuento inferior a las instancias reservadas estándar, pero se pueden cambiar por otra instancia reservada convertible con distintos atributos de instancia. Las instancias reservadas convertibles también se pueden modificar.

Para obtener más información, consulte Tipos de instancias reservadas (clases de oferta).

> **Important**
>
> Una vez que adquiere una instancia reservada, no puede cancelar la compra. Sin embargo, puede modificar, intercambiar o vender la instancia reservada si cambian sus necesidades.

Para obtener más información, consulte la página de Precios de instancias reservadas de Amazon EC2.

instancias reservadas regionales y de zona (alcance)

Cuando se compra una instancia reservada, determina el alcance de la instancia reservada. El alcance es regional o de zona.

- Regional: cuando adquiere una instancia reservada para una región, se denomina instancia reservada regional.
- De zona: al adquirir una instancia reservada para una zona de disponibilidad específica, a esta instancia se la denomina instancia reservada de zona.

El alcance no afecta el precio. Usted paga el mismo precio por un regional o zonal instancia reservada. Para obtener más información acerca de instancia reservada precios, consulte Variables clave que determinan los precios de instancia reservada y Precios de instancias reservadas de Amazon EC2.

Para obtener más información sobre cómo especificar el ámbito de una instancia reservada, consulte Atributos de IR, concretamente el punto Zona de disponibilidad.

Diferencias entre instancias reservadas regionales y de zona

En la siguiente tabla se enumeran algunas de las principales diferencias entre las instancias reservadas regionales y las instancias reservadas de zona:

	instancias reservadas regionales	instancias reservadas de zona
Reservar capacidad	Una instancia reservada regional no reserva capacidad.	Una instancia reservada de zona reserva capacidad en la zona de disponibilidad especificada.
Flexibilidad de zona de disponibilidad	El descuento de la instancia reservada se aplica al uso de la instancia en cualquier zona de disponibilidad de una región especificada.	Sin flexibilidad de zona de disponibilidad — el descuento de la instancia reservada se aplica al uso de la instancia

	instancias reservadas regionales	instancias reservadas de zona
		solo en la zona de disponibilidad especificada.
Flexibilidad del tamaño de instancias	El descuento de instancia reservada se aplica al uso de instancia dentro de la familia de instancias, con independencia del tamaño. Solo se admiten en las instancias reservadas de Amazon Linux/Unix con tenencia predeterminada. Para obtener más información, consulte Flexibilidad del tamaño de la instancia determinada por el factor de normalización.	Sin flexibilidad del tamaño de instancias — el descuento de la instancia reservada se aplica al uso de la instancia solo por el tipo de instancia y tamaño especificado.
Poner en cola una compra	Puede poner en cola las compras de instancias reservadas regionales.	No puede poner en cola las compras de instancias reservadas zonales.

Para obtener más información y ejemplos, consulte Aplicación de las instancias reservadas.

Tipos de instancias reservadas (clases de oferta)

La clase de oferta de un instancia reservada es estándar o convertible. Un estándar instancia reservada proporciona un descuento más significativo que un convertible instancia reservada, pero no se puede intercambiar un estándar instancia reservada. Puede intercambiar convertible instancias reservadas. Puede modificar estándar y convertible instancias reservadas.

La configuración de un instancia reservada comprende un único tipo de instancia, plataforma, alcance y tenencia durante un plazo. Si sus necesidades informáticas cambian, es posible que pueda modificar o intercambiar su instancia reservada.

Diferencias entre estándar y convertible instancias reservadas

A continuación se muestran las diferencias entre estándar y convertible instancias reservadas.

	instancia reservada estándar	Convertible Reserved Instance
Modificar instancias reservadas	Algunos atributos se pueden modificar. Para obtener más información, consulte Modificar instancias reservadas.	Algunos atributos se pueden modificar. Para obtener más información, consulte Modificar instancias reservadas.
Intercambio de instancias reservadas	No se puede intercambiar.	Se puede intercambiar durante el plazo por otra instancia reservada convertible con nuevos atributos, como la familia de instancias, el tipo de instancia, la plataforma, el alcance o la tenencia. Para obtener más información, consulte Intercambiar instancias reservadas convertibles.
Vender en el Marketplace de instancias reservadas	Se puede vender en el Marketplace de instancias reservadas.	No se puede vender en el Marketplace de instancias reservadas.
Comprar en el Marketplace de instancias reservadas	Se puede comprar en el Marketplace de instancias reservadas.	No se puede comprar en el Marketplace de instancias reservadas.

Aplicación de las instancias reservadas

Las instancias reservadas no son instancias físicas, sino más bien un descuento de facturación que se aplica a la ejecución de instancias bajo demanda en su cuenta. Las instancias bajo demanda deben tener determinadas especificaciones de las instancias reservadas para que pueda aprovechar el descuento de facturación.

Si compra una instancia reservada y ya tiene una instancia bajo demanda en ejecución que coincide con las especificaciones de la instancia reservada, el beneficio de facturación se aplica de forma inmediata y automática. No es necesario reiniciar las instancias. Si no tiene una instancia bajo demanda válida en ejecución, lance una instancia bajo demanda con las mismas especificaciones que su instancia reservada. Para obtener más información, consulte Utilizar su instancias reservadas.

La clase de oferta (estándar o convertible) de la instancia reservada no afecta a la forma en que se aplica el descuento de facturación.

Temas

Aplicación de las instancias reservadas de zona

Una instancia reservada que se compra para reservar capacidad en una zona de disponibilidad específica se denomina instancia reservada zonal.

- El descuento de la instancia reservada se aplica al uso compatible de la instancia en dicha zona de disponibilidad.
- Los atributos (tenencia, plataforma, zona de disponibilidad, tipo de instancia y tamaño de instancia) de las instancias en ejecución deben coincidir con los de las instancias reservadas.

Por ejemplo, si adquiere dos instancias reservadas estándar `c4.xlarge` de Linux/Unix con tenencia predeterminada en la zona de disponibilidad us-east-1a, puede haber hasta dos instancias `c4.xlarge` de Linux/Unix con tenencia predeterminada en ejecución en la zona de disponibilidad us-east-1a que se beneficien del descuento por instancia reservada.

Aplicación de las instancias reservadas regionales

Una instancia reservada que se compra para una región se denomina instancia reservada regional y proporciona flexibilidad de zona de disponibilidad y tamaño de la instancia.

- El descuento de la instancia reservada se aplica al uso de la instancia en cualquier zona de disponibilidad en dicha región.

- El descuento de instancia reservada se aplica al uso de instancia dentro de la familia de instancias, con independencia del tamaño. Esto se conoce como flexibilidad de tamaño de instancia.

Flexibilidad del tamaño de instancias

Con la flexibilidad del tamaño instancia, el descuento de instancia reservada se aplica al uso de instancias que tienen la misma familia, generación y atributo. La instancia reservada se aplica desde el tamaño de instancia más pequeño al más grande dentro de la familia de instancias, en función del factor de normalización. Para ver un ejemplo de cómo se aplica el descuento de instancia reservada, consulte Escenario 2: instancias reservadas en una única cuenta mediante el factor de normalización.

Limitaciones

- Permitida: la flexibilidad del tamaño de las instancias solo se admite para las instancias reservadas regionales.
- No permitida: no se admite la flexibilidad del tamaño de las instancias en las siguientes instancias reservadas:
  - instancias reservadas que se adquieren para una zona de disponibilidad específica (instancias reservadas de zona)
  - instancias reservadas para las instancias G4ad, G4dn, G5, G5g, Inf1 e Inf2
  - instancias reservadas para Windows Server, Windows Server con SQL Standard, Windows Server con SQL Server Enterprise, Windows Server con SQL Server Web, RHEL y SUSE Linux Enterprise Server.
  - instancias reservadas con tenencia dedicada

Flexibilidad del tamaño de la instancia determinada por el factor de normalización

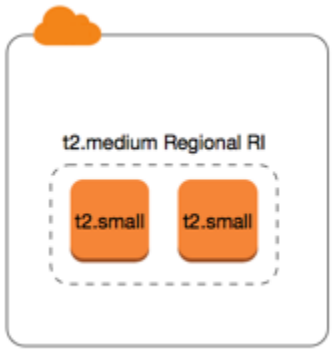
La flexibilidad de tamaño de la instancia está determinada por el factor de normalización del tamaño de la instancia. El descuento se aplica total o parcialmente a las instancias en ejecución de la misma familia de instancias, según el tamaño de instancia de la reserva, en cualquier zona de disponibilidad en la región. Los únicos atributos que deben coincidir son la familia de instancias, la tenencia y la plataforma.

La siguiente tabla describe los diferentes tamaños dentro de una familia de instancias junto con el correspondiente factor de normalización. Esta escala se usa para aplicar la tarifa con descuento de las instancias reservadas al uso normalizado de la familia de instancias.

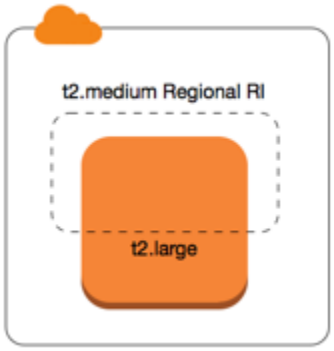
Tamaño de instancia	Factor de normalización
nano	0,25
micro	0,5
small	1
medium	2
large	4
xlarge	8
2xlarge	16
3xlarge	24
4xlarge	32
6xlarge	48
8xlarge	64
9xlarge	72
10xlarge	80
12xlarge	96
16xlarge	128
18xlarge	144
24xlarge	192
32xlarge	256
48xlarge	384
56xlarge	448

Tamaño de instancia	Factor de normalización
112xlarge	896

Por ejemplo, una instancia `t2.medium` tiene un factor de normalización de 2. Si adquiere una instancia reservada de Amazon Linux/Unix con tenencia predeterminada `t2.medium` en la región US East (N. Virginia) y tiene dos instancias `t2.small` en ejecución en su cuenta en dicha región, el beneficio de facturación se aplica en su totalidad a las dos instancias.



O, si tiene una instancia `t2.large` en ejecución en su cuenta en la región US East (N. Virginia), el beneficio de facturación se aplica al 50 % del uso de la instancia.



El factor de normalización también se aplica cuando se modifican las instancias reservadas. Para obtener más información, consulte Modificar instancias reservadas.

Factor de normalización para instancias bare metal

La flexibilidad de tamaño de la instancia también se aplica a instancias bare metal dentro de la familia de instancias. Si tiene instancias reservadas de Amazon Linux/Unix regionales con tenencia compartida en instancias bare metal, puede beneficiarse del ahorro de instancia reservada con la misma familia de instancias. Lo contrario también es cierto: si tiene instancias reservadas de Amazon

Linux/Unix regionales con tenencia compartida en instancias en la misma familia que la instancia bare metal, puede beneficiarse del ahorro de instancia reservada en instancias sin sistema operativo.

Los tamaños de instancia `metal` no tienen un único factor de normalización. Una instancia bare metal tiene el mismo factor de normalización que el tamaño de instancia virtualizado equivalente dentro de la misma familia de instancias. Por ejemplo, una instancia `i3.metal` tiene el mismo factor de normalización que una instancia `i3.16xlarge`.

Tamaño de instancia	Factor de normalización
a1.metal	32
m5zn.metal | x2iezn.metal z1d.metal	96
c6g.metal | c6gd.metal | i3.metal | m6g.metal | m6gd.metal | r6g.metal | r6gd.metal | x2gd.metal	128
c5n.metal	144
c5.metal | c5d.metal | i3en.metal | m5.metal | m5d.metal | m5dn.metal | m5n.metal | r5.metal | r5b.metal | r5d.metal | r5dn.metal | r5n.metal	192
c6i.metal | c6id.metal | m6i.metal | m6id.metal | r6d.metal | r6id.metal	256
u-*.metal	896

Por ejemplo, una instancia `i3.metal` tiene un factor de normalización de 128. Si compra una instancia reservada de Amazon Linux/Unix con tenencia predeterminada `i3.metal` en la US East (N. Virginia), el beneficio de facturación puede aplicarse como se indica a continuación:

- Si tiene una `i3.16xlarge` en ejecución en su cuenta en dicha región, el beneficio de facturación se aplica por completo a la instancia `i3.16xlarge` (factor de normalización `i3.16xlarge` = 128).

- O, si tiene dos instancias `i3.8xlarge` en ejecución en su cuenta en dicha región, el beneficio de facturación se aplica por completo a ambas instancias `i3.8xlarge` (factor de normalización `i3.8xlarge` = 64).
- O, si tiene cuatro instancias `i3.4xlarge` en ejecución en su cuenta en dicha región, el beneficio de facturación se aplica por completo a las cuatro instancias `i3.4xlarge` (factor de normalización `i3.4xlarge` = 32).

Lo opuesto también es cierto. Por ejemplo, si adquiere dos instancias reservadas de Amazon Linux/Unix con tenencia predeterminada `i3.8xlarge` en la US East (N. Virginia) y tiene una instancia `i3.metal` en ejecución en dicha región, el beneficio de facturación se aplica en su totalidad a la instancia `i3.metal`.

Ejemplos de aplicación de instancias reservadas

Los siguientes escenarios cubren las formas en las que se aplican las instancias reservadas.

- Escenario 1: instancias reservadas en una única cuenta
- Escenario 2: instancias reservadas en una única cuenta mediante el factor de normalización
- Escenario 3: instancias reservadas regionales en cuentas vinculadas
- Escenario 4: instancias reservadas regionales en una cuenta vinculada

Escenario 1: instancias reservadas en una única cuenta

Se están ejecutando las siguientes instancias bajo demanda en una cuenta A:

- 4 x instancias con tenencia predeterminada de Linux `m3.large` en la zona de disponibilidad us-east-1a
- 2 x instancias `m4.xlarge` Amazon Linux con tenencia predeterminada en la zona de disponibilidad us-east-1b
- 1 x instancia `c4.xlarge` Amazon Linux con tenencia predeterminada en la zona de disponibilidad us-east-1c

Compra las siguientes instancias reservadas en la cuenta A:

- 4 instancias reservadas `m3.large` de Linux con tenencia predeterminada en la zona de disponibilidad us-east-1a (se reserva la capacidad).

- 4 instancias reservadas `m4.large` de Amazon Linux con tenencia predeterminada en la región us-east-1
- 1 instancias reservadas `c4.large` de Amazon Linux con tenencia predeterminada en la región us-east-1

Los beneficios de la instancia reservada se aplican de la siguiente forma:

- El descuento y la reserva de capacidad de las cuatro instancias reservadas `m3.large` zonales se usan para las cuatro instancias `m3.large` porque los atributos (tamaño de instancia, región, plataforma, tenencia) entre ellas coinciden.
- Las instancias reservadas `m4.large` regionales proporcionan flexibilidad de zona de disponibilidad y de tamaño de instancia, ya que son instancias reservadas de Amazon Linux regionales con tenencia predeterminada.

  Una instancia `m4.large` es equivalente a 4 unidades normalizadas/hora.

  Ha comprado cuatro instancias reservadas `m4.large` regionales y, en total, equivalen a 16 unidades normalizadas/hora (4x4). La cuenta A tiene dos instancias `m4.xlarge` en ejecución, lo que equivale a 16 unidades normalizadas/hora (2x8). En este caso, las cuatro instancias reservadas regionales `m4.large` proporcionan el beneficio de facturación total al uso de las dos instancias `m4.xlarge`.
- La instancia reservada `c4.large` regional de us-east-1 proporciona flexibilidad de zona de disponibilidad y de tamaño de instancia, ya que es una instancia reservada de Amazon Linux regional con tenencia predeterminada y se aplica a la instancia `c4.xlarge`. Una instancia `c4.large` es equivalente a 4 unidades normalizadas/hora y una instancia `c4.xlarge` es equivalente a 8 unidades normalizadas/hora.

  En este caso, la instancia reservada `c4.large` regional proporciona beneficios parciales al uso de instancias `c4.xlarge`. Esto se debe a que la instancia reservada `c4.large` es equivalente a 4 unidades normalizadas/hora de uso, pero la instancia `c4.xlarge` requiere 8 unidades normalizadas/hora. Por consiguiente, el descuento de facturación de la instancia reservada `c4.large` se aplica al 50 % del uso de `c4.xlarge`. El uso restante de `c4.xlarge` se cobra según la tarifa bajo demanda.

Escenario 2: instancias reservadas en una única cuenta mediante el factor de normalización

Se están ejecutando las siguientes instancias bajo demanda en una cuenta A:

- 2 x instancias `m3.xlarge` Amazon Linux con tenencia predeterminada en la zona de disponibilidad us-east-1a
- 2 x instancias `m3.large` Amazon Linux con tenencia predeterminada en la zona de disponibilidad us-east-1b

Compra las siguientes instancias reservadas en la cuenta A:

- 1 x instancia reservada `m3.2xlarge` de Amazon Linux con tenencia predeterminada en la región us-east-1

Los beneficios de la instancia reservada se aplican de la siguiente forma:

- La instancia reservada `m3.2xlarge` regional de us-east-1 proporciona flexibilidad de zona de disponibilidad y de tamaño de instancia, ya que es una instancia reservada de Amazon Linux regional con tenencia predeterminada. Se aplica en primer lugar a las instancias `m3.large` y, a continuación, a las instancias `m3.xlarge`, porque se aplica desde el tamaño de instancia más pequeño al más grande dentro de la familia de instancias según el factor de normalización.

  Una instancia `m3.large` es equivalente a 4 unidades normalizadas/hora.

  Una instancia `m3.xlarge` es equivalente a 8 unidades normalizadas/hora.

  Una instancia `m3.2xlarge` es equivalente a 16 unidades normalizadas/hora.

  El beneficio prestación se aplica de la siguiente manera:

  La instancia reservada `m3.2xlarge` regional proporciona beneficios completos a 2 x `m3.large` uso, porque en conjunto estas instancias representan 8 unidades/hora normalizadas. Esto deja 8 unidades/hora normalizadas para aplicarse a las instancias `m3.xlarge`.

  Con las 8 unidades normalizadas restantes por hora, la instancia reservada `m3.2xlarge` regional proporciona todos los beneficios a 1 x uso de `m3.xlarge`, porque cada instancia `m3.xlarge` es equivalente a 8 unidades normalizadas/hora. El uso restante de `m3.xlarge` se cobra según la tarifa bajo demanda.

Escenario 3: instancias reservadas regionales en cuentas vinculadas

Las instancias reservadas se aplican primero al uso dentro de la cuenta de compra y, a continuación, al uso aplicable en cualquier otra cuenta en la organización. Para obtener más información, consulte instancias reservadas y la facturación unificada. En cuanto a las instancias reservadas regionales que ofrecen flexibilidad de tamaño de las instancias, el beneficio se aplica desde el tamaño de instancia más pequeño al más grande dentro de la familia de instancias.

Se están ejecutando las siguientes instancias bajo demanda en una cuenta A (la cuenta de compra):

- 2 x instancias con tenencia predeterminada de Linux `m4.xlarge` en la zona de disponibilidad us-east-1a
- 1 x instancia con tenencia predeterminada de Linux `m4.2xlarge` en la zona de disponibilidad us-east-1b
- 2 x instancias con tenencia predeterminada de Linux `c4.xlarge` en la zona de disponibilidad us-east-1a
- 1 x instancia con tenencia predeterminada de Linux `c4.2xlarge` en la zona de disponibilidad us-east-1b

Otro cliente está ejecutando las siguientes instancias bajo demanda en la cuenta B — una cuenta vinculada:

- 2 x instancias con tenencia predeterminada de Linux `m4.xlarge` en la zona de disponibilidad us-east-1a

Compra las siguientes instancias reservadas regionales en la cuenta A:

- 4 instancias reservadas `m4.xlarge` de Linux con tenencia predeterminada en la región us-east-1
- 2 instancias reservadas `c4.xlarge` de Linux con tenencia predeterminada en la región us-east-1

Los beneficios de la instancia reservada regional se aplican de la siguiente forma:

- El descuento de las cuatro instancias reservadas `m4.xlarge` lo utilizan las dos instancias `m4.xlarge` y la instancia `m4.2xlarge` única de la cuenta A (la cuenta de compra). Las tres instancias tienen atributos coincidentes (familia de instancia, región, plataforma, tenencia). El descuento se aplica a instancias en la cuenta de compra (cuenta A) primero, incluso aunque la cuenta B (cuenta vinculada) tenga dos `m4.xlarge` que también coinciden con las instancias

reservadas. No hay reserva de capacidad ya que las instancias reservadas son instancias reservadas regionales.

- El descuento de las dos instancias reservadas `c4.xlarge` se aplica a las dos instancias `c4.xlarge`, ya que su tamaño de instancia es más pequeño que el de la instancia `c4.2xlarge`. No hay reserva de capacidad ya que las instancias reservadas son instancias reservadas regionales.

Escenario 4: instancias reservadas regionales en una cuenta vinculada

En general, las instancias reservadas que son propiedad de una cuenta se aplican primero al uso dentro de esa cuenta. No obstante, si hay instancias reservadas sin usar aplicables para una zona de disponibilidad específica (instancias reservadas zonales) en otras cuentas de la organización, se aplicarán a la cuenta antes que las instancias reservadas regionales propiedad de la cuenta. Esto se hace para garantizar un uso máximo de las instancia reservada y una factura reducida. A efectos de facturación, todas las cuentas de la organización se tratan como una sola. El siguiente ejemplo puede ayudar a explicarlo.

Se está ejecutando la siguiente instancia a petición en una cuenta A (la cuenta de compra):

- 1 x instancia con tenencia predeterminada de Linux `m4.xlarge` en la zona de disponibilidad us-east-1a

Un cliente está ejecutando la siguiente instancia a petición en una cuenta B vinculada:

- 1 x instancia con tenencia predeterminada de Linux `m4.xlarge` en la zona de disponibilidad us-east-1b

Compra las siguientes instancias reservadas regionales en la cuenta A:

- 1 instancia reservada `m4.xlarge` de Linux con tenencia predeterminada en la región us-east-1

Un cliente también adquiere las siguientes instancias reservadas zonales en la cuenta C vinculada:

- 1 instancias reservadas `m4.xlarge` de Linux con tenencia predeterminada en la zona de disponibilidad us-east-1a

Los beneficios de la instancia reservada se aplican de la siguiente forma:

- El descuento de la instancia reservada `m4.xlarge` zonal propiedad de la cuenta C se aplica al uso de `m4.xlarge` en la cuenta A.
- El descuento de la instancia reservada `m4.xlarge` regional propiedad de la cuenta A se aplica al uso de `m4.xlarge` en la cuenta B.
- Si la instancia reservada regional propiedad de la cuenta A se aplicó primero al uso en la cuenta A, la instancia reservada zonal propiedad de la cuenta C permanece sin usarse, y el uso en la cuenta B se cobra a las tarifas bajo demanda.

Para obtener más información, consulte la sección sobre instancias reservadas en el informe Billing and Cost Management.

> **Note**
>
> Las instancias reservadas de zona reservan capacidad solo para la cuenta propietaria y no se pueden compartir con otras Cuentas de AWS. Si necesita compartir la capacidad con otras Cuentas de AWS, utilice On-Demand Capacity Reservations.

Utilizar su instancias reservadas

Las instancias reservadas se aplican de forma automática a las instancias bajo demanda en ejecución siempre que las especificaciones coincidan. Si no tiene instancias bajo demanda en ejecución que coincidan con las especificaciones de la instancia reservada, la instancia reservada no se utilizará hasta que lance una instancia con las especificaciones requeridas.

Si va a iniciar una instancia para aprovechar los beneficios de facturación de una instancia reservada, asegúrese de que especifica la siguiente información durante la configuración de la instancia bajo demanda:

Plataforma

Debe especificar una Imagen de máquina de Amazon (AMI) que coincida con la plataforma (descripción del producto) de la instancia reservada. Por ejemplo, si especificó `Linux/UNIX` para la instancia reservada, puede iniciar una instancia desde una AMI de Amazon Linux o una AMI de Ubuntu.

Tipo de instancia

Si ha adquirido una instancia reservada zonal, debe especificar el mismo tipo de instancia que su instancia reservada; por ejemplo, `t3.large`. Para obtener más información, consulte Aplicación de las instancias reservadas de zona.

Si ha adquirido una instancia reservada regional, debe especificar un tipo de instancia de la misma familia de instancias que el tipo de instancia de la instancia reservada. Por ejemplo, si especificó `t3.xlarge` para la instancia reservada, debe iniciar la instancia desde la familia T3, pero puede especificar cualquier tamaño, por ejemplo, `t3.medium`. Para obtener más información, consulte Aplicación de las instancias reservadas regionales.

Zona de disponibilidad

Si ha comprado una instancia reservada zonal para una zona de disponibilidad especifica, debe iniciar la instancia en la misma zona de disponibilidad.

Si ha comprado una instancia reservada regional, puede iniciar la instancia en cualquier zona de disponibilidad en la región que haya especificado para la instancia reservada.

Propiedad

La tenencia (`dedicated` o `shared`) de la instancia debe coincidir con la tenencia de la instancia reservada. Para obtener más información, consulte Dedicated Instances.

Para ver ejemplos sobre cómo se aplican las instancias reservadas a las instancias bajo demanda en ejecución, consulte Aplicación de las instancias reservadas. Para obtener más información, consulte ¿Por qué no se aplican mis instancias reservadas de Amazon EC2 a mi facturación de AWS de la forma que esperaba?

Puede utilizar varios métodos para iniciar las instancias bajo demanda que utilizan el descuento de instancia reservada. Para obtener información acerca de los distintos métodos de inicialización, consulte iniciar la instancia. Puede utilizar Amazon EC2 Auto Scaling para iniciar una instancia. Para obtener más información, consulte la Guía del usuario de Amazon EC2 Auto Scaling.

Cómo se le factura

Todas las instancias reservadas le proporcionan un descuento en comparación con el precio bajo demanda. Con las instancias reservadas paga por todo el plazo independientemente del uso real. Puede elegir pagar por la instancia reservada con un pago inicial, un pago inicial parcial o mensualmente, en función de la opción de pago especificada para la instancia reservada.

Cuando las instancias reservadas caducan, se le cobran las tarifas bajo demanda por el uso de instancias de EC2. Puede poner en cola una instancia reservada para comprarla con tres años por adelantado. Esto contribuirá a garantizar que no sufra una interrupción de la cobertura. Para obtener más información, consulte Poner en cola su compra.

La capa gratuita de AWS está disponible para cuentas nuevas de AWS. Si está utilizando el nivel gratuito de AWS para ejecutar instancias de Amazon EC2 y compra una instancia reservada, se le cobrará de acuerdo con las directrices de precio estándar. Para obtener información, consulte Capa gratuita de AWS.

Contenido

Facturación por uso

Las instancias reservadas se facturan por cada hora de reloj durante el plazo seleccionado, independientemente de si se está ejecutando la instancia. Cada hora de reloj comienza en la hora (cero minutos y cero segundos después de la hora) de un reloj estándar de 24 horas. Por ejemplo, de la 1:00:00 a la 1:59:59 es una hora de reloj. Para obtener más información acerca de los estados de las instancias, consulte Ciclo de vida de la instancia.

El beneficio de facturación de una instancia reservada se aplica a una instancia en ejecución por segundos. La facturación por segundos está disponible para instancias que utilizan una distribución de Linux de código abierto como, por ejemplo, Amazon Linux y Ubuntu. La facturación por hora se utiliza para distribuciones comerciales de Linux como, por ejemplo, Red Hat Enterprise Linux y SUSE Linux Enterprise Server.

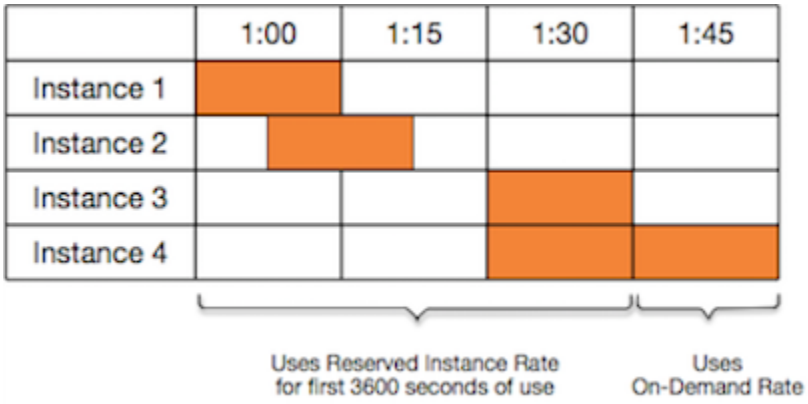
Un beneficio de facturación de instancia reservada puede aplicarse a un máximo de 3600 segundos (una hora) de uso de instancia por hora de reloj. Puede ejecutar al mismo tiempo varias instancias, pero solo puede recibir el beneficio del descuento de instancia reservada por un total de 3600 segundos por hora de reloj; el uso de instancias que supere esos 3600 segundos en una hora de reloj se facturará según la tarifa bajo demanda.

Por ejemplo, si compra una instancia reservada `m4.xlarge` y ejecuta cuatro instancias `m4.xlarge` al mismo tiempo durante una hora, una instancia se cobrará como una hora de uso de instancia

reservada, mientras que las tres instancias restantes se cobrarán como tres horas de uso bajo demanda.

Sin embargo, si compra una instancia reservada `m4.xlarge` y ejecuta cuatro instancias `m4.xlarge` durante 15 minutos (900 segundos) cada una dentro de la misma hora, el tiempo de ejecución total de las instancias será de una hora, lo que supondrá una hora de uso de instancia reservada y 0 horas de uso bajo demanda.

Si hay varias instancias válidas ejecutándose al mismo tiempo, el beneficio de facturación de instancia reservada se aplica a todas las instancias al mismo tiempo hasta un máximo de 3600 segundos de hora de reloj; a partir de ese momento, se aplican tarifas bajo demanda.



La opción Cost Explorer (Explorador de costos) de la consola de Billing and Cost Management le permite analizar los ahorros conseguidos en comparación con la ejecución de instancias bajo demanda. Las preguntas frecuentes sobre las instancias reservadas incluyen un ejemplo de un cálculo de valores de lista.

Si cierra su cuenta de AWS, se detiene la facturación bajo demanda por sus recursos. No obstante, si tiene instancias reservadas en su cuenta, continuará recibiendo una factura por ellas hasta que caduquen.

Visualización de su factura

Encontrará más información sobre los cargos y las cuotas aplicados a su cuenta en la consola de AWS Billing and Cost Management.

- El Dashboard (Panel) muestra un resumen de gastos de la cuenta.
- En la página Bills (Facturas), en Details (Detalles), amplíe la sección Elastic Compute Cloud y la región para obtener información sobre la facturación de las instancias reservadas.

Puede ver los cargos online o puede descargar un archivo CSV.

También puede realizar el seguimiento del uso de la instancia reservada mediante el informe de costo y uso de AWS. Para obtener más información, consulte instancias reservadas en el informe de costos y uso de la Guía del usuario de AWS Billing.

instancias reservadas y la facturación unificada

Los beneficios de precio de las instancias reservadas se comparten cuando la cuenta de adquisición es parte de un conjunto de cuentas facturadas en una sola cuenta del pagador de facturación unificada. El uso de instancias entre todas las cuentas miembro se acumula mensualmente en la cuenta del pagador. Por lo general, esta modalidad es útil para empresas en las que hay diferentes equipos o grupos funcionales; de este modo, se aplica la lógica normal de instancia reservada para calcular la factura. Para obtener más información, consulte Facturación unificada para AWS Organizations.

Si cierra la cuenta que compró la instancia reservada, se cobrará dicha instancia en la cuenta del pagador hasta que se venza. Luego de que la cuenta cerrada se elimine de forma permanente al cabo de los 90 días, las cuentas miembro dejan de beneficiarse del descuento en la facturación de la instancia reservada.

> **Note**
>
> Las instancias reservadas de zona reservan capacidad solo para la cuenta propietaria y no se pueden compartir con otras Cuentas de AWS. Si necesita compartir la capacidad con otras Cuentas de AWS, utilice On-Demand Capacity Reservations.

Capas de precios de descuento por instancia reservada

Si su cuenta reúne los requisitos para una capa de precios de descuento, automáticamente recibe descuentos en las cuotas de pago adelantado o de uso de instancias para las adquisiciones de instancia reservada que realice dentro de ese nivel de capa a partir de ese punto. Para poder optar a un descuento, el valor de lista de las instancias reservadas de la región debe ser de 500 000 USD o más.

Se aplican las siguientes reglas:

- Las capas de precios y los descuentos relacionados solo se aplican a las compras de instancias reservadas estándar de Amazon EC2.
- Las capas de precios no se aplican a las instancias reservadas para Windows con SQL Server Standard, SQL Server Web y SQL Server Enterprise.
- Las capas de precios no se aplican a las instancias reservadas para Linux con SQL Server Standard, SQL Server Web y SQL Server Enterprise.
- Los descuentos de capas de precios solo se aplican a compras realizadas desde AWS. No se aplican a compras de instancias reservadas de terceros.
- Las capas de precios de descuento no se pueden aplicar actualmente a compras de instancia reservada convertible.

Temas

Calcular instancia reservada descuentos en precios

Para determinar la capa de precios de su cuenta, calcule el valor de lista de todas las instancias reservadas en una región. Multiplique el precio recurrente por hora de cada reserva por el número total de horas del plazo y sume el precio inicial sin descuento (también conocido como precio fijo) en el momento de la compra. Como el valor de lista se basa en un precio (público) sin descuento, no se ve afectado si usted cumple con los requisitos para un descuento por volumen o si el precio cae después de la adquisición de las instancias reservadas.

```
List value = fixed price + (undiscounted recurring hourly price * hours in term)
```

Por ejemplo, en el caso de una instancia reservada `t2.small` con un pago inicial parcial de 1 año, supongamos que el precio del pago inicial sea de 60,00 USD y que la tarifa por hora sea de 0,007 USD. Esto proporciona un valor de lista de 121,32 USD.

```
121.32 = 60.00 + (0.007 * 8760)
```

New console

Para ver los valores de precio fijo de las instancias reservadas mediante la consola de Amazon EC2

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Reserved Instances (instancias reservadas).
3. Para mostrar la columna Precio inicial, seleccione la configuración () en la esquina superior derecha, active Precio inicial y seleccione Confirmar.

Old console

Para ver los valores de precio fijo de las instancias reservadas mediante la consola de Amazon EC2

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Reserved Instances (instancias reservadas).
3. Para mostrar la columna Precio inicial, seleccione la configuración () en la esquina superior derecha, seleccione Precio inicial y seleccione Cerrar.

Para ver los valores de precio fijo de las instancias reservadas mediante la línea de comandos

- describe-reserved-instances (AWS CLI)
- Get-EC2ReservedInstance (AWS Tools for Windows PowerShell)
- DescribeReservedInstances (API de Amazon EC2)

Comprar con una capa de descuento

Cuando se compran instancias reservadas, Amazon EC2 aplica automáticamente cualquier descuento a la parte de la compra que se encuentre dentro de una capa de precios de descuento. No es necesario hacer nada de forma diferente; y se pueden comprar instancias reservadas utilizando la herramienta de Amazon EC2 que se desee. Para obtener más información, consulte Comprar instancias reservadas.

Después de que el valor de lista de las instancias reservadas activas de una región pase a otra capa de precios de descuento, todas las compras futuras de las instancias reservadas en dicha región se cobrarán con una tarifa con descuento. Si una única compra de instancias reservadas en una región supera el umbral de una capa de descuento, la porción de la compra situada por debajo del umbral de precio se cobrará a la tarifa con descuento. Para obtener más información sobre los ID temporales de instancia reservada que se crean durante el proceso de compra, consulte Cruce de capas de precios.

Si el valor de lista cae por debajo del precio de esa capa de precios de descuento —por ejemplo, si alguna de las instancias reservadas caduca— no se aplicará descuento a las compras futuras de instancias reservadas en la región. Sin embargo, continuará obteniendo el descuento que se aplica a las instancias reservadas adquiridas originalmente dentro de la capa de precios de descuento.

Al comprar instancias reservadas hay cuatro posibles escenarios:

- Ningún descuento — la compra dentro de una región aún está por debajo del umbral de descuento.
- Descuento parcial — la compra dentro de una región cruza el umbral de la primera capa de descuentos. No se aplica ningún descuento a una o más reservas, y la tarifa con descuento se aplica a las reservas restantes.
- Descuento completo — toda la compra de una región cae dentro de una capa de descuento y el descuento se aplica correctamente.
- Dos tarifas de descuento — la compra dentro de una región pasa de una capa de descuento inferior a una capa de descuento superior. Se le cobran dos tarifas diferentes: una o más reservas a la tarifa con descuento inferior y el resto de las reservas a la tarifa con descuento superior.

Cruce de capas de precios

Si su compra cruza a una capa de precios con descuento, verá varias entradas para esa compra: una para la parte de la compra que se cobra al precio normal y otra para la parte de la compra que se compra a la tarifa con descuento aplicable.

El servicio de instancia reservada genera varios ID de instancia reservada porque la compra cruzó de una capa sin descuento o desde una capa con descuento a otra. Existe un ID para cada conjunto de reservas en una capa. En consecuencia, el ID devuelto por el comando de la CLI o la acción de la API de la compra es diferente del ID real de las nuevas instancias reservadas.

Facturación unificada para capas de precios

Una cuenta de facturación unificada acumula el valor de lista de las cuentas miembro de una región. Cuando el valor de lista de todas las instancias reservadas activas para la cuenta de facturación consolidada alcanza una capa de precios de descuento, todas las instancias reservadas que se compren después de este momento por cualquiera de los miembros de la cuenta de facturación consolidada se cobrarán a la tarifa con descuento (siempre que el valor de lista para esa cuenta consolidada se mantenga por encima del umbral de la capa de precios de descuento). Para obtener más información, consulte instancias reservadas y la facturación unificada.

Comprar instancias reservadas

Para comprar una instancia reservada, busque ofertas de instancia reservada de AWS y de vendedores externos, ajustando los parámetros de búsqueda hasta que encuentre exactamente lo que esté buscando.

Cuando busca instancias reservadas para comprarlas, recibe un presupuesto con el costo de las ofertas devueltas. Cuando se realiza la compra, AWS asigna automáticamente un precio límite al precio de compra. El costo total de las instancias reservadas no superará el importe del presupuesto.

Si el precio sube o cambia por algún motivo, la compra no se completará. Cuando compra una instancia reservada de un vendedor externo en el Marketplace de instancia reservada de EC2 , si existen ofertas similares a la que ha elegido pero a un precio inicial inferior, AWS le venderá las ofertas al precio inicial inferior.

Antes de confirmar la compra, revise los detalles de la instancia reservada que tiene previsto comprar y asegúrese de que todos los parámetros sean correctos. Después de comprar una instancia reservada (a un vendedor externo en el Marketplace de instancias reservadas o a AWS), no puede cancelar la compra.

Para comprar y modificar instancias reservadas, asegúrese de que su usuario tenga los permisos adecuados, como la capacidad de describir zonas de disponibilidad. Para obtener más información, consulte the section called “Trabajar con Instancias reservadas” (API) o the section called “Trabajar con Instancias reservadas” (consola).

Temas

Selección de una plataforma

Amazon EC2 admite las siguientes plataformas para instancias reservadas:

- Linux/UNIX
- Linux con SQL Server Standard
- Linux con SQL Server Web
- Linux con SQL Server Enterprise
- SUSE Linux
- Red Hat Enterprise Linux
- Red Hat Enterprise Linux con alta disponibilidad
- Windows
- Windows con SQL Server Standard
- Windows con SQL Server Web
- Windows con SQL Server Enterprise

Al adquirir una instancia reservada, debe elegir una oferta para una plataforma que represente el sistema operativo de la instancia.

instancias de Linux

- Para las distribuciones SUSE Linux y RHEL, debe elegir ofertas para esas plataformas específicas, es decir, para las plataformas SUSE Linux o Red Hat Enterprise Linux.
- En el resto de distribuciones de Linux (incluida Ubuntu), elija una oferta para la plataforma Linux/UNIX.
- Si trae su propia suscripción RHEL existente, debe elegir una oferta para plataforma Linux/UNIX, no una oferta para la plataforma Red Hat Enterprise Linux.

instancias de Windows

- En Windows con SQL Standard, Windows con SQL Server Enterprise y Windows con SQL Server Web, debe elegir ofertas para estas plataformas específicas.
- En las demás versiones de Windows, elija una oferta para la plataforma Windows.

> **Note**
>
> Ubuntu Pro no está disponible como instancia reservada. Para obtener ahorros significativos en comparación con los precios de las instancias bajo demanda, le recomendamos que utilice Ubuntu Pro con Savings Plans. Para obtener más información, consulte la Guía del usuario de Savings Plans.

> **Important**
>
> Si prevé adquirir una instancia reservada para aplicar a una instancia bajo demanda iniciada desde una AMI de AWS Marketplace, verifique primero el campo `PlatformDetails` de la AMI. El campo `PlatformDetails` indica qué instancia reservada comprar. Los detalles de la plataforma de la AMI deben coincidir con la plataforma de la instancia reservada, de lo contrario la instancia reservada no se aplicará a la instancia a petición. Para obtener información sobre cómo ver los detalles de la plataforma de la AMI, consulte Comprender la información de facturación de la AMI.

Poner en cola su compra

De forma predeterminada, cuando compra un instancia reservada, la compra se realiza inmediatamente. No obstante, puede poner sus compras en una cola con una hora y fecha futuras. Por ejemplo, puede poner una compra en una cola para la fecha aproximada en la que vencerá una instancia reservada existente. Esto contribuirá a garantizar que no sufra una interrupción de la cobertura.

Puede poner compras en cola para instancias reservadas regionales, pero no instancias reservadas zonales ni instancias reservadas de otros vendedores. Puede poner en cola una compra con hasta tres años por adelantado. En la hora y fecha deseadas, la compra se realiza con el método de pago predeterminado. Una vez que el pago se completa correctamente, se aplica el beneficio de facturación.

Puede ver sus compras en cola en la consola de Amazon EC2. El estado de una compra en cola es queued (en cola). Puede cancelar las compras en cola en cualquier momento antes de su horario programado. Para obtener más información, consulte Cancelar una compra en cola.

Comprar Estándar instancias reservadas

Puede comprar instancias reservadas estándar en una zona de disponibilidad específica y obtener una reserva de capacidad. O bien, puede renunciar a la reserva de capacidad y comprar una instancia reservada estándar regional.

New console

Para comprar instancias reservadas estándar mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Reserved Instances (instancias reservadas) y, a continuación, elija Purchase instancias reservadas (Compra de instancias reservadas).
3. En Offering class (Clase de oferta), elija Standard (Estándar) para mostrar las instancias reservadas estándar.
4. Para comprar una reserva de capacidad, active Only show offerings that reserve capacity (Solo se muestran las ofertas para reservar capacidad) en la esquina superior derecha de la pantalla de compra. Al activar esta configuración, aparece el campo Availability Zone (Zona de disponibilidad).

   Para comprar un instancia reservada regional, desactive esta configuración. Cuando desactiva esta configuración, desaparece el campo Availability Zone (Zona de disponibilidad).

5. Seleccione otras configuraciones según sea necesario y, a continuación, elija Search (Buscar).
6. Para cada uno de los instancia reservada que quiera comprar, introduzca la cantidad deseada y seleccione Add to Cart (Agregar al carrito).

   Para comprar una instancia reservada estándar en el Marketplace de instancias reservadas, busque 3rd Party (Terceros) en la columna Seller (Vendedor) en los resultados de búsqueda. La columna Term (Plazo) muestra plazos que no son estándar. Para obtener más información, consulte Comprar en el Marketplace de instancia reservada.
7. Para ver un resumen de las instancias reservadas que ha seleccionado, elija View cart (Ver carrito).
8. Si Order on (Pedir el) es Now (Ahora), la compra se completa inmediatamente después de seleccionar Order all (Pedir todo). Para poner una compra en cola, elija Now (Ahora) y seleccione una fecha. Es posible seleccionar fechas diferentes para cada oferta elegible en el carrito de la compra. La compra se pone en cola hasta las 00:00 UTC de la fecha seleccionada.
9. Para completar el pedido, elija Order all (Pedir todo).

   Si, en el momento de realizar el pedido, existen ofertas similares a su elección pero con un precio inferior, AWS le venderá las ofertas al precio inferior.
10. Elija Close (Cerrar).

    El estado del pedido se muestra en la columna State (Estado). Cuando se complete el pedido, el valor de State (Estado) cambia de `Payment-pending` a `Active`. Cuando el estado de la instancia reservada sea `Active`, está lista para usar.

> **Note**
>
> Si el estado es `Retired`, es posible que AWS no haya recibido el pago.

Old console

Para comprar instancias reservadas estándar mediante la consola

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

2. En el panel de navegación, elija Reserved Instances (instancias reservadas) y, a continuación, elija Purchase instancias reservadas (Compra de instancias reservadas).
3. En Offering Class (Clase de oferta), elija Standard (Estándar) para mostrar las instancias reservadas estándar.
4. Para comprar una reserva de capacidad, elija Only show offerings that reserve capacity (Solo se muestran las ofertas para reservar capacidad) en la esquina superior derecha de la pantalla de compra. Para comprar una instancia reservada regional, deje la casilla desactivada.
5. Seleccione otras configuraciones según sea necesario y elija Search (Buscar).

   Para comprar una instancia reservada estándar en el Marketplace de instancias reservadas, busque 3rd Party (Terceros) en la columna Seller (Vendedor) en los resultados de búsqueda. La columna Term (Plazo) muestra plazos que no son estándar.
6. Para cada uno de los instancia reservada que quiera comprar, introduzca la cantidad y seleccione Add to Cart (Agregar al carrito).
7. Para ver un resumen de las instancias reservadas que ha seleccionado, elija View Cart (Ver carrito).
8. Si Order On (Pedir el) es Now (Ahora), la compra se completa inmediatamente. Para poner una compra en cola, elija Now (Ahora) y seleccione una fecha. Es posible seleccionar fechas diferentes para cada oferta elegible en el carrito de la compra. La compra se pone en cola hasta las 00:00 UTC de la fecha seleccionada.
9. Para completar el pedido, elija Order (Pedir).

   Si, en el momento de realizar el pedido, existen ofertas similares a su elección pero con un precio inferior, AWS le venderá las ofertas al precio inferior.
10. Elija Close (Cerrar).

    El estado del pedido se muestra en la columna State (Estado). Cuando se complete el pedido, el valor de State (Estado) cambia de `payment-pending` a `active`. Cuando el estado de la instancia reservada sea `active`, está lista para usar.

> **Note**
>
> Si el estado es `retired`, es posible que AWS no haya recibido el pago.

Comprar una instancia reservada estándar mediante AWS CLI

1. Busque las instancias reservadas disponibles con el comando describe-reserved-instances-offerings. Especifique `standard` para que el parámetro `--offering-class` solo devuelva instancias reservadas estándar. Puede aplicar parámetros adicionales para acotar los resultados. Por ejemplo, si desea comprar una instancia reservada `t2.large` regional con una tenencia predeterminada para `Linux/UNIX` para un período de 1 año exclusivamente:

```
aws ec2 describe-reserved-instances-offerings \
    --instance-type t2.large \
    --offering-class standard \
    --product-description "Linux/UNIX" \
    --instance-tenancy default \
    --filters Name=duration,Values=31536000 Name=scope,Values=Region
```

   Para encontrar instancias reservadas en el Marketplace exclusivo para instancias reservadas, utilice el filtro `marketplace` y no especifique una duración en la solicitud, ya que el plazo puede ser inferior a 1 o 3 años.

```
aws ec2 describe-reserved-instances-offerings \
    --instance-type t2.large \
    --offering-class standard \
    --product-description "Linux/UNIX" \
    --instance-tenancy default \
    --filters Name=marketplace,Values=true
```

   Cuando encuentre una instancia reservada que satisfaga sus necesidades, anote el ID de la oferta. Por ejemplo:

```
"ReservedInstancesOfferingId": "bec624df-a8cc-4aad-a72f-4f8abc34caf2"
```

2. Ejecute el comando purchase-reserved-instances-offering para comprar la instancia reservada. Tiene que especificar el ID de la oferta de instancia reservada que obtuvo en el paso anterior así como el número de instancias para la reserva.

```
aws ec2 purchase-reserved-instances-offering \
    --reserved-instances-offering-id bec624df-a8cc-4aad-a72f-4f8abc34caf2 \
    --instance-count 1
```

De forma predeterminada, la compra se completa inmediatamente. Tiene la opción de poner la compra en cola añadiendo el siguiente parámetro a la llamada anterior.

```
--purchase-time "2020-12-01T00:00:00Z"
```

3. Ejecute el comando describe-reserved-instances para obtener el estado de la instancia reservada.

```
aws ec2 describe-reserved-instances
```

También puede usar los siguientes comandos de las AWS Tools for Windows PowerShell:

- Get-EC2ReservedInstancesOffering
- New-EC2ReservedInstance
- Get-EC2ReservedInstance

Una vez que se completa la compra, si ya tiene una instancia en ejecución que coincide con las especificaciones de la instancia reservada, el beneficio de facturación se aplica de forma inmediata. No es necesario reiniciar las instancias. Si no tiene una instancia en ejecución apropiada, lance una instancia y asegúrese de que coincida con los mismos criterios que especificó para la instancia reservada. Para obtener más información, consulte Utilizar su instancias reservadas.

Para ver ejemplos sobre cómo se aplican las instancias reservadas a las instancias en ejecución, consulte Aplicación de las instancias reservadas.

Comprar instancias reservadas convertibles

Puede comprar instancias reservadas convertibles en una zona de disponibilidad específica y obtener una reserva de capacidad. O bien, puede renunciar a la reserva de capacidad y comprar una instancia reservada convertible regional.

New console

Para comprar instancias reservadas convertibles mediante la consola

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

2. En el panel de navegación, elija Reserved Instances (instancias reservadas) y, a continuación, elija Purchase instancias reservadas (Compra de instancias reservadas).
3. En Offering class (Clase de oferta), elija Convertible (Convertibles) para visualizar las instancias reservadas convertibles.
4. Para comprar una reserva de capacidad, active Only show offerings that reserve capacity (Solo se muestran las ofertas para reservar capacidad) en la esquina superior derecha de la pantalla de compra. Al activar esta configuración, aparece el campo Availability Zone (Zona de disponibilidad).

   Para comprar un instancia reservada regional, desactive esta configuración. Cuando desactiva esta configuración, desaparece el campo Availability Zone (Zona de disponibilidad).
5. Seleccione otras configuraciones según sea necesario y elija Search (Buscar).
6. Para cada uno de los instancia reservada convertible que quiera comprar, introduzca la cantidad y seleccione Add to cart (Agregar al carrito).
7. Para ver un resumen de la selección, elija View cart (Ver carrito).
8. Si Order on (Pedir el) es Now (Ahora), la compra se completa inmediatamente después de seleccionar Order all (Pedir todo). Para poner una compra en cola, elija Now (Ahora) y seleccione una fecha. Es posible seleccionar fechas diferentes para cada oferta elegible en el carrito de la compra. La compra se pone en cola hasta las 00:00 UTC de la fecha seleccionada.
9. Para completar el pedido, elija Order all (Pedir todo).

   Si, en el momento de realizar el pedido, existen ofertas similares a su elección pero con un precio inferior, AWS le venderá las ofertas al precio inferior.
10. Elija Close (Cerrar).

    El estado del pedido se muestra en la columna State (Estado). Cuando se complete el pedido, el valor de State (Estado) cambia de `Payment-pending` a `Active`. Cuando el estado de la instancia reservada sea `Active`, está lista para usar.

> **Note**
>
> Si el estado es `Retired`, es posible que AWS no haya recibido el pago.

Old console

Para comprar instancias reservadas convertibles mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Reserved Instances (instancias reservadas) y, a continuación, elija Purchase instancias reservadas (Compra de instancias reservadas).
3. En Offering Class (Clase de oferta), elija Convertible (Convertibles) para visualizar las instancias reservadas convertibles.
4. Para comprar una reserva de capacidad, elija Only show offerings that reserve capacity (Solo se muestran las ofertas para reservar capacidad) en la esquina superior derecha de la pantalla de compra. Para comprar una instancia reservada regional, deje la casilla desactivada.
5. Seleccione otras configuraciones según sea necesario y elija Search (Buscar).
6. Para cada uno de los instancia reservada convertible que quiera comprar, introduzca la cantidad y seleccione Add to Cart (Agregar al carrito).
7. Para ver un resumen de la selección, elija View Cart (Ver carrito).
8. Si Order On (Pedir el) es Now (Ahora), la compra se completa inmediatamente. Para poner una compra en cola, elija Now (Ahora) y seleccione una fecha. Es posible seleccionar fechas diferentes para cada oferta elegible en el carrito de la compra. La compra se pone en cola hasta las 00:00 UTC de la fecha seleccionada.
9. Para completar el pedido, elija Order (Pedir).

   Si, en el momento de realizar el pedido, existen ofertas similares a su elección pero con un precio inferior, AWS le venderá las ofertas al precio inferior.
10. Elija Close (Cerrar).

    El estado del pedido se muestra en la columna State (Estado). Cuando se complete el pedido, el valor de State (Estado) cambia de `payment-pending` a `active`. Cuando el estado de la instancia reservada sea `active`, está lista para usar.

> **Note**
>
> Si el estado es `retired`, es posible que AWS no haya recibido el pago.

Comprar una instancia reservada convertible mediante AWS CLI

1. Busque las instancias reservadas disponibles con el comando describe-reserved-instances-offerings. Especifique `convertible` para que el parámetro `--offering-class` solo devuelva instancias reservadas convertibles. Puede aplicar parámetros adicionales para reducir los resultados; por ejemplo, si desea comprar una instancia reservada `t2.large` regional con tenencia predeterminada de `Linux/UNIX`:

   ```
   aws ec2 describe-reserved-instances-offerings \
       --instance-type t2.large \
       --offering-class convertible \
       --product-description "Linux/UNIX" \
       --instance-tenancy default \
       --filters Name=scope,Values=Region
   ```

   Cuando encuentre una instancia reservada que satisfaga sus necesidades, anote el ID de la oferta. Por ejemplo:

   ```
   "ReservedInstancesOfferingId": "bec624df-a8cc-4aad-a72f-4f8abc34caf2"
   ```

2. Ejecute el comando purchase-reserved-instances-offering para comprar la instancia reservada. Tiene que especificar el ID de la oferta de instancia reservada que obtuvo en el paso anterior así como el número de instancias para la reserva.

   ```
   aws ec2 purchase-reserved-instances-offering \
       --reserved-instances-offering-id bec624df-a8cc-4aad-a72f-4f8abc34caf2 \
       --instance-count 1
   ```

   De forma predeterminada, la compra se completa inmediatamente. Tiene la opción de poner la compra en cola añadiendo el siguiente parámetro a la llamada anterior.

   ```
   --purchase-time "2020-12-01T00:00:00Z"
   ```

3. Ejecute el comando describe-reserved-instances para obtener el estado de la instancia reservada.

   ```
   aws ec2 describe-reserved-instances
   ```

También puede usar los siguientes comandos de las AWS Tools for Windows PowerShell:

- Get-EC2ReservedInstancesOffering
- New-EC2ReservedInstance
- Get-EC2ReservedInstance

Si ya tiene una instancia en ejecución que coincide con las especificaciones de la instancia reservada, el beneficio de facturación se aplica de forma inmediata. No es necesario reiniciar las instancias. Si no tiene una instancia en ejecución apropiada, lance una instancia y asegúrese de que coincida con los mismos criterios que especificó para la instancia reservada. Para obtener más información, consulte Utilizar su instancias reservadas.

Para ver ejemplos sobre cómo se aplican las instancias reservadas a las instancias en ejecución, consulte Aplicación de las instancias reservadas.

Comprar en el Marketplace de instancia reservada

Puede comprar instancias reservadas de vendedores externos propietarios de instancias reservadas que ya no necesitan en el Marketplace de instancias reservadas. Para ello, puede usar la consola de Amazon EC2 o una herramienta de línea de comandos. El proceso es similar a la compra de instancias reservadas desde AWS. Para obtener más información, consulte Comprar Estándar instancias reservadas.

Existen algunas diferencias entre las instancias reservadas compradas en el Marketplace de instancias reservadas y las instancias reservadas compradas directamente en AWS:

- Plazo: a las instancias reservadas que se compran a vendedores externos les queda menos del plazo estándar. Los plazos estándar completos que ofrece AWS son de uno o tres años.
- Precio inicial: las instancias reservadas de terceros se pueden vender a precios iniciales diferentes. Las tarifas de uso o recurrentes son las mismas que se establecieron al adquirir originalmente las instancias reservadas de AWS.
- Tipos de instancias reservadas: las instancias reservadas estándar de Amazon EC2 solo se pueden comprar en el Marketplace de instancias reservadas. Las instancias reservadas convertibles y las instancias reservadas de Amazon RDS y Amazon ElastiCache no están disponibles para su compra en el Marketplace de instancias reservadas.

Cierta información básica sobre usted se compartirá con el vendedor como, por ejemplo, información sobre el país y el código postal.

Esta información permite a los vendedores calcular cualquier impuesto de transacción necesario que deban remitir al gobierno (como el impuesto sobre las ventas o sobre el valor añadido) y se proporciona como un informe de desembolso. En circunstancias excepcionales, es posible que AWS tuviera que proporcionar al vendedor su dirección de correo electrónico, para que pueda ponerse en contacto con usted sobre preguntas relacionadas con la venta (por ejemplo, por temas fiscales).

Por el mismo motivo, AWS comparte el nombre de la entidad legal del vendedor en la factura de compra del comprador. Si necesita información adicional sobre el vendedor, por motivos fiscales o por algún motivo similar, contacte con AWS Support.

Ver instancias reservadas

Puede ver las instancias reservadas que ha comprado mediante la consola de Amazon EC2 o con una herramienta de línea de comandos.

Para ver sus instancias reservadas en la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Reserved Instances (instancias reservadas).
3. Aparece una lista con las instancias reservadas en cola, activas y retiradas. La columna State (Estado) muestra el estado.
4. Si es un vendedor en el Marketplace de instancias reservadas, la pestaña My Listings (Mis listados) muestra el estado de una reserva que aparece en una lista del Marketplace de instancias reservadas. Para obtener más información, consulte Estados del listado de instancia reservada.

Para ver sus instancias reservadas utilizando la línea de comandos

- describe-reserved-instances (AWS CLI)
- Get-EC2ReservedInstance (Herramientas para Windows PowerShell)

Cancelar una compra en cola

Puede poner en cola una compra con hasta tres años por adelantado. Puede cancelar las compras en cola en cualquier momento antes de su horario programado.

New console

Para cancelar una compra en cola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Reserved Instances (instancias reservadas).
3. Seleccione una o varias instancias reservadas.
4. Elija Actions (Acciones), Delete queued Reserved Instances (Eliminar instancias reservadas en la cola).
5. Cuando se le pida confirmación, elija Delete (Eliminar) y, a continuación, Close (Cerrar).

Old console

Para cancelar una compra en cola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Reserved Instances (instancias reservadas).
3. Seleccione una o varias instancias reservadas.
4. Elija Actions (Acciones), Delete Queued Reserved Instances (Eliminar instancias reservadas en la cola).
5. Cuando se le indique que confirme, seleccione Yes, Delete.

Para cancelar una compra en cola mediante la línea de comandos

- delete-queued-reserved-instances (AWS CLI)
- Remove-EC2QueuedReservedInstance (Herramientas para Windows PowerShell)

Renovar un instancia reservada

Puede renovar una instancia reservada antes de que esté programado para caducar. La renovación de una instancia reservada pone en cola la compra de una instancia reservada con la misma configuración hasta que la instancia reservada actual caduque.

New console

Para renovar una instancia reservada con una compra en cola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Reserved Instances (instancias reservadas).
3. Seleccione la instancia reservada que desea renovar.
4. Elija Acciones, Renovar instancias reservadas.
5. Para completar el pedido, elija Order all (Pedir todo) y, a continuación, Close (Cerrar).

Old console

Para renovar una instancia reservada con una compra en cola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Reserved Instances (instancias reservadas).
3. Seleccione la instancia reservada que desea renovar.
4. Elija Acciones, Renovar instancias reservadas.
5. Para completar el pedido, elija Order (Pedir).

Vender en el Marketplace de instancias reservadas

El Marketplace de instancias reservadas es una plataforma que admite la venta de instancias reservadas estándar no utilizadas de terceros y de clientes de AWS, que pueden variar en plazos y opciones de precios. Por ejemplo, es posible que quiera vender instancias reservadas después de mover instancias a una nueva región de AWS, cambiar a un nuevo tipo de instancia, finalizar proyectos antes de que expiren, cuando cambien las necesidades de su empresa o si tiene una capacidad que no necesita.

En cuanto incluya las instancias reservadas en el Marketplace de instancias reservadas, estas estarán disponibles para que los compradores potenciales puedan encontrarlas. Todas las instancias reservadas están agrupadas de acuerdo con la duración del plazo restante y el precio por hora.

Para atender la solicitud de un comprador de comprar una instancia reservada de un vendedor externo a través del Marketplace de instancia reservada de EC2, AWS primero vende la Instancia reservada con el precio inicial más bajo en la agrupación especificada. A continuación, AWS vende las instancias reservadas con el siguiente precio más bajo, hasta que se haya completado

la totalidad del pedido del comprador. Después, AWS procesa las transacciones y transfiere la propiedad de las instancias reservadas al comprador.

Usted es el propietario de la instancia reservada hasta que la vende. Después de la venta, usted renuncia a la reserva de la capacidad y a las cuotas recurrentes con descuento. Si continúa usando la instancia, AWS le cobrará el precio bajo demanda a partir del momento en que se vendió la instancia reservada.

Si desea vender sus instancias reservadas no utilizadas en el Marketplace de instancias reservadas, debe cumplir determinados requisitos.

Para obtener más información acerca de la compra de instancias reservadas en el Marketplace de instancias reservadas, consulte Comprar en el Marketplace de instancia reservada.

Contenido

Restricciones y limitaciones

Para poder vender las reservas que tenga sin utilizar, debe registrarse como vendedor en el Marketplace de instancias reservadas. Para obtener información, consulte Registrarse como vendedor.

Cuando se venden instancias reservadas se aplican las siguientes limitaciones y restricciones:

- Solo se pueden vender instancias reservadas regionales y zonales estándar de Amazon EC2 en el Mercado de instancias reservadas.

- No se pueden vender instancias reservadas convertibles de Amazon EC2 en el Mercado de instancias reservadas.
- Las instancias reservadas para otros servicios de AWS, como Amazon RDS y Amazon ElastiCache, no se pueden vender en el Mercado de instancias reservadas.
- Debe quedar como mínimo un mes en el plazo de la instancia reservada estándar.
- No puede vender una instancia reservada estándar en una región que esté deshabilitada de forma predeterminada.
- El precio mínimo permitido en el Marketplace de instancias reservadas es de 0,00 USD.
- Puede vender instancias reservadas sin pago inicial, con pago inicial parcial o con pago total por adelantado en el marketplace de instancias reservadas siempre que hayan estado activas en su cuenta durante al menos 30 días. Además, si hay un pago inicial en una instancia reservada, solo se puede vender después de que AWS ha recibido el pago inicial.
- No puede modificar su cotización directamente en el Marketplace de instancias reservadas. No obstante, puede cambiar su listado cancelándolo primero y, a continuación, creando otro listado con nuevos parámetros. Para obtener información, consulte Determinar el precio de su instancias reservadas. También puede modificar instancias reservadas antes de incluirlas en la lista. Para obtener información, consulte Modificar instancias reservadas.
- AWS cobra una cuota de servicio del 12 por ciento del precio inicial total de cada instancia reservada estándar que usted venda en el Marketplace de instancias reservadas. El precio inicial es el precio que el vendedor cobra por la instancia reservada estándar.
- Cuando se registra como vendedor, el banco que especifique debe tener una dirección de EE. UU. Para obtener más información, consulte Requisitos adicionales del vendedor para productos de pago en la Guía del vendedor de AWS Marketplace.
- Los clientes de Amazon Web Services India Private Limited (AWS India) no pueden vender las instancias reservadas en el Marketplace de instancias reservadas, incluso si cuentan con una cuenta bancaria en EE. UU. Para obtener más información, consulte ¿Cuáles son las diferencias entre las Cuentas de AWS y las cuentas de AWS India?

Registrarse como vendedor

> **Note**
>
> Únicamente Usuario raíz de la cuenta de AWS puede registrar una cuenta como vendedor.

Para vender en el Marketplace de instancias reservadas, primero debe registrarse como vendedor. Durante el registro, debe proporcionar la siguiente información:

- Información bancaria:AWS debe tener su información bancaria para que podamos ingresar los fondos cuando vendamos sus reservas. El banco que especifique debe tener una dirección en Estados Unidos. Para obtener más información, consulte Cuenta bancaria para abonos.
- Información fiscal — todos los vendedores deben pasar una entrevista sobre información fiscal para determinar las obligaciones fiscales a las que están sujetos. Para obtener más información, consulte Información fiscal.

Después de que AWS reciba su registro de vendedor completado, recibirá un correo electrónico confirmando su registro e informando que puede comenzar a vender en el Marketplace de instancias reservadas.

Cuenta bancaria para abonos

AWS debe tener su información bancaria para que podamos ingresar los fondos cuando vendamos su instancia reservada. El banco que especifique debe tener una dirección en Estados Unidos. Para obtener más información, consulte Requisitos adicionales del vendedor para productos de pago en la Guía del vendedor de AWS Marketplace.

Para registrar una cuenta bancaria predeterminada para desembolsos

1. Abra la página de registro de vendedores del Marketplace de instancias reservadas e inicie sesión usando sus credenciales de AWS.
2. En la página Manage Bank Account (Administrar cuenta bancaria), proporcione la siguiente información sobre el banco en el que desea recibir los pagos:
   - Nombre del titular de la cuenta bancaria
   - Número de ruta
   - Número de cuenta
   - Tipo de cuenta de banco

> **Note**
>
> Si está usando una cuenta bancaria corporativa, se le solicitará que envíe la información acerca de la cuenta bancaria a por fax (1-206-765-3424).

Después del registro, la cuenta bancaria proporcionada se establece como predeterminada, pendiente de verificación con el banco. Puede tomar hasta dos semanas verificar una nueva cuenta bancaria, tiempo durante el cual no podrá recibir desembolsos. Para una cuenta establecida, normalmente se tarda unos dos días en completar los desembolsos.

Para cambiar la cuenta bancaria predeterminada para desembolsos

1. En la página de Registro de vendedores del Marketplace de instancias reservadas, inicie sesión con la cuenta que utilizó al registrarse.
2. En la página Manage Bank Account (Administrar cuenta bancaria), añada una nueva cuenta bancaria o modifique la cuenta bancaria predeterminada según sea necesario.

Información fiscal

La venta de instancias reservadas podría estar sujeta a impuestos basados en transacciones, como un impuesto sobre las ventas o un impuesto sobre el valor añadido. Debería consultar con el departamento fiscal, legal, financiero o contable de su negocio para determinar si se deben aplicar impuestos transaccionales. Usted es responsable de recaudar y enviar los impuestos basados en transacciones a la autoridad fiscal adecuada.

Como parte del proceso de registro de vendedor, debe realizar una entrevista sobre impuestos en el portal de registro de vendedores. La entrevista recopila su información fiscal y rellena un formulario W-9, W-8BEN o W-8BEN-E del IRS, que se utiliza para determinar las obligaciones fiscales necesarias.

La información fiscal que debe introducir como parte de la entrevista sobre impuestos puede variar en función de si trabaja de forma individual o como empresa, y de si su negocio es una persona o entidad estadounidense o no. Cuando rellene la entrevista sobre impuestos, recuerde lo siguiente:

- La información proporcionada por AWS, incluida la información en este tema, no constituye asesoramiento fiscal, legal ni otro tipo de asesoramiento profesional. Para averiguar cómo podrían

afectar los requisitos de información del IRS a su negocio o si tiene cualquier otra pregunta, póngase en contacto con su asesor fiscal, legal u otro tipo de asesor profesional.

- Para cumplir con los requisitos de información del IRS de la forma más eficiente posible, responda a todas las preguntas y escriba toda la información solicitada durante la entrevista.
- Compruebe sus respuestas. Evite los errores ortográficos o escribir números de identificación fiscal incorrectos. Pueden dar como resultado un formulario fiscal invalidado.

En función de las respuestas de su entrevista sobre impuestos y los umbrales de notificación del IRS, Amazon puede presentar el formulario 1099-K. Amazon envía una copia de su formulario 1099-K el 31 de enero o antes del año siguiente al año en que su cuenta de impuestos alcance los niveles de umbral. Por ejemplo, si su cuenta de impuestos alcanza el umbral en 2018, se le enviará por correo el formulario 1099-K el 31 de enero de 2019 o antes.

Para obtener más información sobre los requisitos del IRS y el formulario 1099-K, consulte el sitio web del IRS.

Determinar el precio de su instancias reservadas

A la hora de fijar el precio de las instancias reservadas, tenga en cuenta lo siguiente:

- Precio inicial: el precio inicial es el único que puede especificar para la instancia reservada que está vendiendo. El precio inicial es el único pago que el comprador realiza cuando compra una instancia reservada.

  Dado que, de forma predeterminada, el valor de las instancias reservadas va disminuyendo a lo largo del tiempo, AWS puede establecer la disminución de los precios en incrementos iguales mes a mes. No obstante, usted puede establecer diferentes precios iniciales en función de cuándo se venda su reserva. Por ejemplo, si a su instancia reservada le quedan nueve meses del plazo, puede especificar el importe que aceptaría si un cliente quisiera comprar dicha instancia reservada a la que quedan nueve meses. Podría fijar otro precio para cuando quedaran cinco meses, e incluso otro precio para cuando quedara un mes.

  El precio mínimo permitido en el Marketplace de instancias reservadas es de 0,00 USD.
- Límites: los siguientes límites para la venta de instancias reservadas se aplican a la vida útil de su Cuenta de AWS. No son límites anuales.
  - Puede vender hasta 50 000 USD en instancias reservadas.
  - Puede vender hasta 5000 instancias reservadas.

Por lo general, estos límites no se pueden aumentar, pero se evaluará caso por caso si se solicita. Para solicitar un aumento de los límites, complete el formulario de aumento de los límites de servicio. En Tipo de límite, elija Ventas de instancias reservadas de EC2.

- No se puede modificar: no puede modificar su listado directamente. No obstante, puede cambiar su listado cancelándolo primero y, a continuación, creando otro listado con nuevos parámetros.
- Se puede cancelar: puede cancelar su listado en cualquier momento, siempre que esté en el estado `active`. No puede cancelar el listado si ya se ha encontrado una coincidencia o se está procesando para una venta. Si ya se ha encontrado alguna coincidencia para algunas de las instancias de su listado y usted cancela el listado, solo se eliminarán del listado las instancias que tengan una coincidencia.

Enumerar su instancias reservadas

Como vendedor registrado, puede elegir vender una o más de sus instancias reservadas. Puede elegir venderlas todas en un listado o en partes. Además, puede incluir en la lista instancias reservadas con cualquier configuración de tipo de instancia, plataforma y ámbito.

La consola determina un precio sugerido. Comprueba las ofertas que coinciden con su instancia reservada y busca la del menor precio. De no encontrarla, calcula un precio sugerido en función del coste de la instancia reservada durante su tiempo restante. Si el valor calculado es inferior a 1,01 $, el precio sugerido es 1,01 $.

Si cancela su listado y una parte de dicho listado ya se ha vendido, la cancelación no será efectiva en la parte vendida. Solo la parte que no se haya vendido de la cotización dejará de estar disponible en el Marketplace de instancias reservadas.

Publicar una instancia reservada en el Marketplace de instancias reservadas mediante AWS Management Console

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Reserved Instances (instancias reservadas).
3. Seleccione las instancias reservadas que desee mostrar y elija Actions (Acciones) y Sell instancias reservadas (Vender instancias reservadas).
4. En la página Configure Your instancia reservada Listing (Configurar su listado de instancias reservadas), defina el número de instancias que desea vender y el precio inicial para el plazo restante en las columnas correspondientes. Para ver cómo cambia el valor de su reserva a lo

largo del tiempo restante del plazo, seleccione la flecha junto a la columna Months Remaining (Meses restantes).

5. Si es un usuario avanzado y desea personalizar los precios, puede escribir diferentes valores en los siguientes meses. Para regresar a la bajada de precios lineal predeterminada, elija Reset (Restablecer).
6. Elija Continue (Continuar) cuando haya terminado de configurar el listado.
7. Confirme los detalles del listado, en la página Confirm Your instancia reservada Listing (Confirmar su listado de instancia reservada) y, si está satisfecho, elija List Reserved Instance (Mostrar instancia reservada).

Para ver los listados en la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Reserved Instances (instancias reservadas).
3. Seleccione la instancia reservada mostrada y elija la pestaña My Listings (Mis listados) que encontrará en la parte inferior de la página.

Administrar instancias reservadas en el Marketplace de instancias reservadas mediante AWS CLI

1. Obtenga una lista de las instancias reservadas mediante el comando describe-reserved-instances.
2. Anote el ID de la instancia reservada que desee incluir en el listado y llame a create-reserved-instances-listing. Debe especificar el ID de la instancia reservada, el número de instancias y el plan de precios.
3. Para ver el listado, use el comando describe-reserved-instances-listings.
4. Para cancelar el listado, use el comando cancel-reserved-instances-listings.

Estados del listado de instancia reservada

La opción Listing State (Estado de listados) de la pestaña My Listings (Mis listados) de la página de instancias reservadas muestra el estado actual de sus listados:

La información que se muestra en Listing State (Estado de listados) es relativa al estado su listado en el Marketplace de instancias reservadas. Es una información distinta de la información de

estado que se muestra en la columna State (Estado) de la página Reserved Instances (instancias reservadas). La información que se muestra en la columna State (Estado) es sobre la reserva.

- active (activo) — el listado está disponible para su compra.
- canceled (cancelado): el listado se ha cancelado y no está disponible para su compra en el Marketplace de instancias reservadas.
- closed (cerrado) — la instancia reservada no aparece en la lista. Una instancia reservada podría tener el estado `closed` porque la venta del listado se ha completado.

Ciclo de vida de un listado

Cuando todas las instancias del listado han encontrado comprador y se han vendido, la pestaña My Listings (Mis listados) muestra que Total instance count (Número total de instancias) coincide con el recuento que aparece bajo Sold (Vendido). Además, no queda ninguna instancia Available (Disponible) en el listado y su Status (Estado) es `closed`.

Cuando solo se ha vendido una parte del listado, AWS retira las instancias reservadas de este y crea una cantidad de instancias reservadas igual al de las instancias reservadas que quedan en el recuento. De esta manera, el ID del listado y el listado al que representa, que ahora ofrece menos reservas para la venta, siguen activos.

Cualquier venta futura de instancias reservadas de este listado se procesará de esta manera. Cuando todas las instancias reservadas del listado se hayan vendido, AWS marcará el listado como `closed`.

Por ejemplo, se crea un listado ID de listado de instancias reservadas 5ec28771-05ff-4b9b-aa31-9e57dexample con 5 elementos.

La pestaña My Listings (Mis listados) de la página de la consola Reserved Instances (instancias reservadas) muestra el listado de la siguiente forma:

ID de listado de instancia reservada 5ec28771-05ff-4b9b-aa31-9e57dexample

- Total reservation count = 5
- Sold = 0
- Available = 5
- Status = active

Un comprador adquiere dos de las reservas, lo que deja un recuento de tres reservas aún disponibles para su venta. Debido a esta venta parcial, AWS crea una nueva reserva con un recuento de tres que representa las reservas que aún están a la venta.

Este es el aspecto que tendría el listado en la pestaña My Listings (Mis listados):

ID de listado de instancia reservada 5ec28771-05ff-4b9b-aa31-9e57dexample

- Total reservation count = 5
- Sold = 2
- Available = 3
- Status = active

Si cancela su listado y una parte del listado ya se ha vendido, la cancelación no será efectiva en la parte vendida. Solo la parte que no se haya vendido de la cotización dejará de estar disponible en el Marketplace de instancias reservadas.

Después de vender la instancia reservada

Después de que se haya vendido la instancia reservada, AWS le enviará una notificación por correo electrónico. Cada día que se produce algún tipo de actividad, usted recibe una notificación por correo electrónico donde se recopilan todas las actividades del día. Estas actividades pueden ser la creación o la venta de un listado o el envío de fondos por parte de AWS a su cuenta.

Para hacer un seguimiento del estado de un listado de instancia reservada a través de la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Reserved Instances (instancias reservadas).
3. Elija la pestaña My Listings (Mis listados).

   La pestaña My Listings (Mis listados) contiene el valor Listing State (Estado de listados). También contiene información sobre el plazo, el precio del listado y un desglose de cuántas instancias del listado están disponibles, pendientes, vendidas y canceladas.

También puede usar el comando describe-reserved-instances-listings con el filtro adecuado para obtener información sobre los listados.

Recibir los pagos

En cuanto AWS reciba el dinero del comprador, se enviará un mensaje al correo electrónico de la cuenta del propietario registrado sobre la instancia reservada vendida.

AWS envía una transferencia bancaria de la Automated Clearing House (ACH, Cámara de compensación automatizada) a su cuenta bancaria. Normalmente, esta transferencia se realiza entre uno y tres días después de la venta de la instancia reservada. Los abonos se realizan una vez al día. Recibirá un correo electrónico con un informe de abonos una vez liberados los fondos. Recuerde que no puede recibir ningún abono hasta que AWS reciba la verificación de su banco. Esto puede tardar hasta dos semanas.

La instancia reservada que ha vendido seguirá apareciendo cuando describa las instancias reservadas.

Recibirá un desembolso en efectivo por sus instancias reservadas mediante transferencia bancaria directa a su cuenta bancaria. AWS cobra una cuota de servicio del 12 por ciento del precio inicial total de cada instancia reservada que usted venda en el Marketplace de instancias reservadas.

Información compartida con el comprador

Cuando usted vende en el Marketplace de instancias reservadas, AWS comparte el nombre legal de su empresa en la declaración del comprador de acuerdo con la legislación de Estados Unidos. Además, si el comprador llama a AWS Support porque necesita contactar con usted para una factura o por algún motivo relacionado con los impuestos, es posible que AWS deba proporcionar al comprador su dirección de email a fin de que pueda contactar directamente con usted.

Por razones similares, en el informe del desembolso proporcionamos al vendedor la información sobre el país y el código postal del comprador. Como vendedor, podría necesitar esta información para acompañar cualquier impuesto de transacción necesario que deba remitir al gobierno (como el impuesto sobre las ventas o sobre el valor añadido).

AWS no puede ofrecer asesoramiento fiscal, pero si su experto fiscal determina que necesita información adicional específica, contacte con AWS Support.

Modificar instancias reservadas

Cuando cambien sus necesidades, puede modificar su Estándar o instancias reservadas convertibles y seguir disfrutando de los beneficios de facturación. Puede modificar atributos como la zona de disponibilidad, el tamaño de la instancia (dentro de la misma familia de instancias y generación) y el ámbito de su instancia reservada.

> **Note**
>
> También se puede intercambiar una instancia reservada convertible por otra instancia reservada convertible con una configuración diferente. Para obtener más información, consulte Intercambiar instancias reservadas convertibles.

Se pueden modificar todas las instancias reservadas o un subconjunto de ellas. Puede separar las instancias reservadas originales en dos o más instancias reservadas nuevas. Por ejemplo, si tiene una reserva para 10 instancias en `us-east-1a` y decide mover 5 instancias a `us-east-1b`, la solicitud de modificación da como resultado dos nuevas reservas: una para 5 instancias en `us-east-1a` y la otra para 5 instancias en `us-east-1b`.

También puede fusionar dos o más instancias reservadas en una única instancia reservada. Por ejemplo, si tiene cuatro instancias reservadas `t2.small` de una instancia cada una, puede fusionarlas para crear una instancia reservada `t2.large`. Para obtener más información, consulte Compatibilidad para modificar tamaños de instancia.

Después de la modificación, el beneficio de las instancias reservadas se aplica únicamente a las instancias que coincidan con los nuevos parámetros. Por ejemplo, si cambia la zona de disponibilidad de una reserva, la reserva de capacidad y los beneficios de precios se aplican automáticamente al uso de la instancia en la nueva zona de disponibilidad. Las instancias que ya no coincidan con los nuevos parámetros se cambian a la tarifa bajo demanda a menos que la cuenta disponga de otras reservas aplicables.

Si la solicitud de modificación se realiza correctamente:

- La reserva modificada entra en vigor inmediatamente y el beneficio de precio se aplica a las nuevas instancias comenzando a contar desde la hora de la solicitud de modificación. Por ejemplo, si modifica correctamente sus reservas a las 21:15 h, el beneficio de precio se transfiere a su nueva instancia a las 21 h. Puede obtener la fecha de entrada en vigor de las instancias reservadas modificadas usando el comando describe-reserved-instances.
- Se retira la reserva original. Su fecha de finalización es la fecha de inicio de la nueva reserva, mientras que la fecha de finalización de la nueva reserva es la misma que la fecha de finalización de la instancia reservada original. Si modifica una reserva de tres años a la que aún le quedaban 16 meses de plazo, la reserva modificada resultante es una reserva de 16 meses con la misma fecha de finalización que la reserva original.
- La reserva modificada muestra un precio fijo de 0 USD y no el precio fijo de la reserva original.

- El precio fijo de la reserva modificada no afecta a los cálculos de capa de precios de descuento aplicados a su cuenta, que se basan en el precio fijo de la reserva original.

Si la solicitud de modificación genera un error, las instancias reservadas conservan su configuración original y, de forma inmediata, estarán disponibles para otra solicitud de modificación.

No se le cobra ninguna cuota por la modificación y usted no recibe ninguna factura nueva.

Puede modificar sus reservas siempre que lo desee, pero no puede cambiar ni cancelar una solicitud de modificación pendiente después de enviarla. Cuando la modificación se haya completado correctamente, podrá enviar otra solicitud de modificación para revertir cualquiera de los cambios que haya hecho, si fuera necesario.

Contenido

Requisitos y restricciones a modificar

Puede modificar estos atributos como se indica a continuación.

Atributo modificable	Plataformas admitidas	Limitaciones y considera ciones
Cambiar zonas de disponibi lidad dentro de la misma región	Linux y Windows	-
Cambiar el ámbito de zona de disponibilidad a región y viceversa.	Linux y Windows	Una instancia reservada zonal se asigna a una zona de disponibilidad y reserva capacidad en esa zona de disponibilidad. Si cambia el ámbito de zona de disponibi

Atributo modificable	Plataformas admitidas	Limitaciones y considera ciones
		lidad a región (es decir, de zonal a regional), pierde el beneficio de reserva de capacidad. Una instancia reservada regional se asigna a una región. Su descuento de instancia reservada se puede aplicar a instancias que se ejecutan en cualquier zona de disponibilidad de esa región. Además, el descuento de instancias reservadas se aplica al uso de instancias en todos los tamaños de la familia de instancias seleccion ada. Si cambia el ámbito de región a zona de disponibi lidad (es decir, de regional a zonal), pierde la flexibilidad de la zona de disponibilidad y la flexibilidad del tamaño de la instancia (si corresponde). Para obtener más informaci ón, consulte Aplicación de las instancias reservadas.

Atributo modificable	Plataformas admitidas	Limitaciones y considera ciones
Cambiar el tamaño de instancia dentro de la misma familia de instancias y generación	Solo Linux/UNIX La flexibilidad del tamaño de instancia no está disponibl e para instancias reservada s en otras plataformas, como Linux con SQL Server Standard, Linux con SQL Server Web, Linux con SQL Server Enterprise, Red Hat Enterprise Linux, SUSE Linux, Windows, Windows con SQL Standard, Windows con SQL Server Enterprise y Windows con SQL Server Web.	La reserva debe utilizar la tenencia predeterminada. Algunas familias de instancias no se admiten porque no hay ningún otro tamaño disponibl e. Para obtener más informaci ón, consulte Compatibilidad para modificar tamaños de instancia

Requisitos

Amazon EC2 procesa su solicitud de modificación si hay suficiente capacidad para su configuración de destino (si procede) y si se cumplen las siguientes condiciones:

- La instancia reservada no se puede modificar antes o al mismo tiempo que la compra
- La instancia reservada debe estar activa
- No puede ser una solicitud de modificación pendiente
- La instancia reservada no aparece en el Marketplace de instancias reservadas.
- Debe haber una coincidencia entre la huella del tamaño de la instancia de la reserva original y la nueva configuración. Para obtener más información, consulte Compatibilidad para modificar tamaños de instancia.
- Las instancias reservadas originales son todas instancias reservadas estándar o todas instancias reservadas convertibles, no algunas de cada tipo
- Las instancias reservadas originales deben caducar dentro de la misma hora, si son instancias reservadas estándar

- La instancia reservada no es una instancia G4, G4ad, G4dn, G5, G5g, Inf1 o Inf2.

Compatibilidad para modificar tamaños de instancia

Puede modificar el tamaño de una instancia reservada si se cumplen los siguientes requisitos.

Requisitos

- La plataforma es Linux/UNIX.
- Debe seleccionar otro tamaño de instancia de la misma familia de instancias (indicado con una letra, por ejemplo, T) y generación (indicado con un número, por ejemplo, 2).

  Por ejemplo, puede modificar una instancia reservada de `t2.small` a `t2.large` porque ambas pertenecen a la misma familia y generación de T2. Sin embargo, no puede modificar una instancia reservada de T2 a M2 o de T2 a T3 porque, en ambos ejemplos, la generación y la familia de instancias de destino no son las mismas que las de la instancia reservada original.
- No se puede modificar el tamaño de las instancias reservadas en el caso de las siguientes instancias, ya que cada una tiene un solo tamaño:
  - `t1.micro`
- No se puede modificar el tamaño de las instancias reservadas en el caso de las siguientes combinaciones de familia, generación y atributos de instancias:
  - G4ad
  - G4dn
  - G5
  - G5g
  - Inf1
  - Inf2
- Las instancia reservada original y nueva deben tener la misma huella del tamaño de instancia.

Contenido

- Huella del tamaño de instancia
- Factores de normalización para instancias bare metal

Huella del tamaño de instancia

Cada instancia reservada tiene una huella del tamaño de instancia, que se determina mediante el factor de normalización del tamaño de instancia y el número de instancias de la reserva. Cuando modifica los tamaños de instancia en instancia reservada, la huella de la nueva configuración debe coincidir con la de la configuración original, en caso contrario no se procesará la solicitud de modificación.

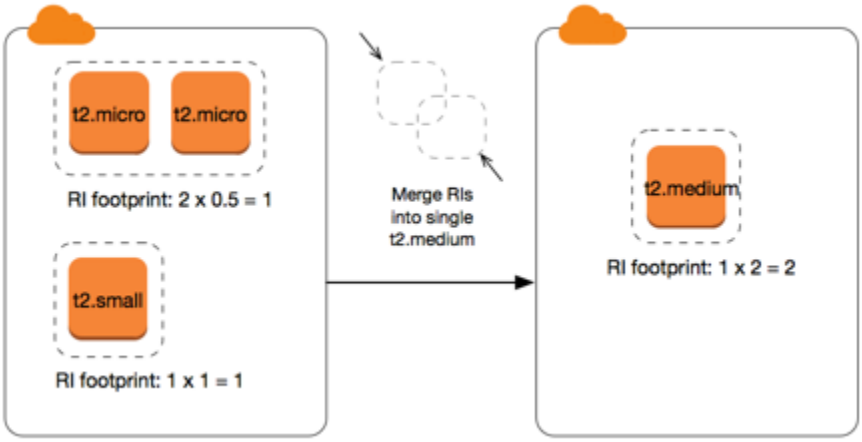
Para calcular la huella del tamaño de instancia de una instancia reservada, multiplique el número de instancias por el factor de normalización. En la consola de Amazon EC2, el factor de normalización se mide en unidades. En la tabla siguiente se describe el factor de normalización para los tamaños de instancia de una familia de instancias. Por ejemplo, `t2.medium` tiene un factor de normalización de 2 por lo que una reserva de cuatro instancias `t2.medium` tiene una huella de 8 unidades.

Tamaño de instancia	Factor de normalización
nano	0,25
micro	0,5
small	1
medium	2
large	4
xlarge	8
2xlarge	16
3xlarge	24
4xlarge	32
6xlarge	48
8xlarge	64
9xlarge	72
10xlarge	80

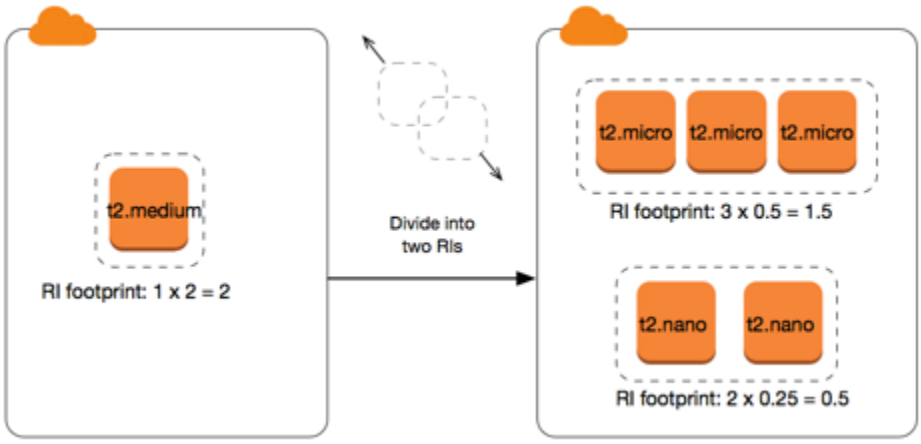
Tamaño de instancia	Factor de normalización
12xlarge	96
16xlarge	128
18xlarge	144
24xlarge	192
32xlarge	256
48xlarge	384
56xlarge	448
112xlarge	896

Se pueden asignar las reservas a diferentes tamaños de instancia dentro de la misma familia de instancia, siempre que la huella del tamaño de instancia de la reserva siga siendo la misma. Por ejemplo, puede dividir una reserva para una instancia `t2.large` (1 en 4 unidades) en cuatro instancias `t2.small` (4 en 1 unidad). Del mismo modo, puede combinar una reserva para cuatro instancias `t2.small` en una instancia `t2.large`. Sin embargo, no puede cambiar la reserva para dos instancias `t2.small` en una instancia `t2.large` porque la huella de la nueva reserva (4 unidades) es mayor que la huella de la reserva original (2 unidades).

En el ejemplo siguiente, tiene una reserva con dos instancias `t2.micro` (1 unidad) y una reserva con una instancia `t2.small` (1 unidad). Si fusiona ambas reservas en una sola reserva con una instancia `t2.medium` (2 unidades), la huella de la nueva reserva es igual a la huella de las reservas combinadas.



También puede modificar una reserva para dividirla en dos o más reservas. En el siguiente ejemplo, se tiene una reserva con una instancia `t2.medium` (2 unidades). Puede dividir la reserva en dos reservas, una con dos instancias `t2.nano` (0,5 unidades) y la otra con tres instancias `t2.micro` (1,5 unidades).



Factores de normalización para instancias bare metal

Puede modificar una reserva con instancias `metal` mediante otros tamaños dentro de la misma familia de instancias. Del mismo modo, puede modificar una reserva con instancias que no sean instancias bare metal mediante el tamaño de `metal` dentro de la misma familia de instancias. Por lo general, una instancia bare metal tiene el mismo tamaño que el de la instancia más grande disponible dentro de la misma familia de instancias. Por ejemplo, una instancia `i3.metal` tiene el mismo tamaño que una instancia `i3.16xlarge`, por tanto tienen el mismo factor de normalización.

En la siguiente tabla se describe el factor de normalización para los tamaños de instancia bare metal en las familias de instancias que tienen instancias bare metal. El factor de normalización de instancias `metal` depende de la familia de instancias, a diferencia de los otros tamaños de instancia.

Tamaño de instancia	Factor de normalización
a1.metal	32
m5zn.metal | x2iezn.metal z1d.metal	96
c6g.metal | c6gd.metal | i3.metal | m6g.metal | m6gd.metal | r6g.metal | r6gd.metal | x2gd.metal	128
c5n.metal	144
c5.metal | c5d.metal | i3en.metal | m5.metal | m5d.metal | m5dn.metal | m5n.metal | r5.metal | r5b.metal | r5d.metal | r5dn.metal | r5n.metal	192
c6i.metal | c6id.metal | m6i.metal | m6id.metal | r6d.metal | r6id.metal	256
u-*.metal	896

Por ejemplo, una instancia `i3.metal` tiene un factor de normalización de 128. Si compra una instancia reservada de Amazon Linux/Unix con tenencia predeterminada `i3.metal`, puede dividir la reserva como se indica a continuación:

- Una instancia `i3.16xlarge` tiene el mismo tamaño que una instancia `i3.metal`, por tanto su factor de normalización es 128 (128/1). La reserva para una instancia `i3.metal` se puede modificar en una instancia `i3.16xlarge`.
- Una instancia `i3.8xlarge` tiene la mitad de tamaño que una instancia `i3.metal`, por tanto su factor de normalización es 64 (128/2). La reserva para una instancia `i3.metal` se puede dividir en dos instancias `i3.8xlarge`.
- Una instancia `i3.4xlarge` tiene un cuarto del tamaño de una instancia `i3.metal`, por tanto su factor de normalización es 32 (128/4). La reserva para una instancia `i3.metal` se puede dividir en cuatro instancias `i3.4xlarge`.

Enviar solicitudes de modificación

Antes de modificar las instancias reservadas, asegúrese de haber leído las restricciones aplicables. Antes de modificar el tamaño de instancia, calcule la huella del tamaño de instancia total de las reservas originales que desea modificar y asegúrese también de que coincide con la huella del tamaño de instancia total de las nuevas configuraciones.

New console

Modificar sus instancias reservadas mediante AWS Management Console

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la página Reserved Instances (instancias reservadas), seleccione las instancias reservadas que desee modificar y elija Actions (Acciones), Modify Reserved Instances (Modificar instancias reservadas).

   > **Note**
   >
   > Si las instancias reservadas no se encuentran en estado activo o no se pueden modificar, la opción Modify instancias reservadas (Modificar instancias reservadas) está deshabilitada.

3. La primera entrada de la tabla de modificación muestra atributos de las instancias reservadas seleccionadas y, como mínimo, una configuración de destino debajo de ellas. La columna Units (Unidades) muestra la huella del tamaño de instancia total. Seleccione Add (Añadir) para cada nueva configuración que desee añadir. Modifique los atributos según sea necesario para cada configuración.

   - Scope (Ámbito): elija si la configuración se aplica a una zona de disponibilidad o a toda la región.
   - Availability Zone (Zona de disponibilidad): elija la zona de disponibilidad requerida. No es aplicable para instancias reservadas regionales.
   - Tipo de instancia: seleccione el tipo de instancia necesario. Las configuraciones combinadas deben ser iguales a la huella de tamaño de instancia de las configuraciones originales.
   - Count (Recuento): especifique el número de instancias. Para dividir las instancias reservadas en varias configuraciones, reduzca el recuento, elija Add (Añadir) y especifique un recuento para la configuración adicional. Por ejemplo, si tiene una única configuración

con un recuento de 10, puede cambiar su recuento a 6 y añadir una configuración con un recuento de 4. Este proceso retira la instancia reservada original después de activar la nueva instancias reservadas.

4. Elija Continue.
5. Para confirmar sus opciones de modificación cuando termine de especificar las configuraciones de destino, elija Submit modifications (Enviar modificaciones).
6. Puede determinar el estado de la solicitud de modificación fijándose en la columna State (Estado) de la pantalla de instancias reservadas. A continuación se muestran los posibles estados.

   - active (activa) (modificación pendiente) — Estado de transición para instancias reservadas originales
   - retired (retirada) (modificación pendiente) — Estado de transición para instancias reservadas originales mientras se crean instancias reservadas nuevas
   - retired (retirada) — instancias reservadas modificada y reemplazada correctamente
   - active (activa) — Una de las siguientes:
     - instancias reservadas nuevas creadas a partir de una solicitud de modificación realizada correctamente
     - instancias reservadas originales después de una solicitud de modificación errónea

Old console

Modificar sus instancias reservadas mediante AWS Management Console

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la página Reserved Instances (instancias reservadas), seleccione las instancias reservadas que desee modificar y elija Actions (Acciones), Modify Reserved Instances (Modificar instancias reservadas).

> **Note**
>
> Si las instancias reservadas no se encuentran en estado activo o no se pueden modificar, la opción Modify instancias reservadas (Modificar instancias reservadas) está deshabilitada.

3. La primera entrada de la tabla de modificación muestra atributos de las instancias reservadas seleccionadas y, como mínimo, una configuración de destino bajo ellas. La columna Units (Unidades) muestra la huella del tamaño de instancia total. Seleccione Add (Añadir) para cada nueva configuración que desee añadir. Modifique los atributos según sea necesario para cada configuración y elija Continue (Continuar):

   - Scope (Ámbito): elija si la configuración se aplica a una zona de disponibilidad o a toda la región.
   - Availability Zone (Zona de disponibilidad): elija la zona de disponibilidad requerida. No es aplicable para instancias reservadas regionales.
   - Tipo de instancia: seleccione el tipo de instancia necesario. Las configuraciones combinadas deben ser iguales a la huella de tamaño de instancia de las configuraciones originales.
   - Count (Recuento): especifique el número de instancias. Para dividir las instancias reservadas en varias configuraciones, reduzca el recuento, elija Add (Añadir) y especifique un recuento para la configuración adicional. Por ejemplo, si tiene una única configuración con un recuento de 10, puede cambiar su recuento a 6 y añadir una configuración con un recuento de 4. Este proceso retira la instancia reservada original después de activar la nueva instancias reservadas.
4. Para confirmar sus opciones de modificación cuando termine de especificar las configuraciones de destino, elija Submit Modifications (Enviar modificaciones).
5. Puede determinar el estado de la solicitud de modificación fijándose en la columna State (Estado) de la pantalla de instancias reservadas. A continuación se muestran los posibles estados.

   - active (activa) (modificación pendiente) — Estado de transición para instancias reservadas originales
   - retired (retirada) (modificación pendiente) — Estado de transición para instancias reservadas originales mientras se crean instancias reservadas nuevas
   - retired (retirada) — instancias reservadas modificada y reemplazada correctamente
   - active (activa) — Una de las siguientes:
     - instancias reservadas nuevas creadas a partir de una solicitud de modificación realizada correctamente
     - instancias reservadas originales después de una solicitud de modificación errónea

Para modificar sus instancias reservadas utilizando la línea de comandos

1. Para modificar sus instancias reservadas, puede usar uno de los siguientes comandos:
   - modify-reserved-instances (AWS CLI)
   - Edit-EC2ReservedInstance (AWS Tools for Windows PowerShell)
2. Para obtener el estado de la modificación(`processing`, `fulfilled` o `failed`), utilice uno de los siguientes comandos:
   - describe-reserved-instances-modifications (AWS CLI)
   - Get-EC2ReservedInstancesModification (AWS Tools for Windows PowerShell)

Solucionar problemas de solicitudes de modificación

Si los valores de la configuración de destino que solicitó eran únicos, se recibe un mensaje que indica que se está procesando la solicitud. En este punto, Amazon EC2 solo ha determinado que los parámetros de la solicitud de modificación son válidos. A pesar de ello, aún es posible que la solicitud de modificación genere algún error debido a falta de capacidad disponible.

En algunas situaciones, podría recibir un mensaje indicando que las solicitudes de modificación no se han completado o han generado un error en lugar de una confirmación. Use la información que le proporcionan esos mensajes como punto de partida para volver a enviar otra solicitud de modificación. Asegúrese de haber leído las restricciones aplicables antes de enviar la solicitud.

No todas las instancias reservadas seleccionadas se pueden procesar para una modificación

Amazon EC2 identifica y enumera las instancias reservadas que no se pueden modificar. Si recibe un mensaje como este, vaya a la página Instancias reservadas en la consola de Amazon EC2 y compruebe la información para las instancias reservadas.

Error al procesar la solicitud de modificación

Se enviaron una o varias instancias reservadas para su modificación y no se puede procesar ninguna de las solicitudes. Según el número de reservas que se están modificando, puede recibir diferentes versiones del mensaje.

Amazon EC2 muestra los motivos por los que no se puede procesar su solicitud. Por ejemplo, podría haber especificado la misma configuración de destino —una combinación de zona de disponibilidad y plataforma— para uno o más subconjuntos de las instancias reservadas que se están modificando. Pruebe a volver a enviar las solicitudes de modificación pero asegúrese de que

los detalles de instancia de las reservas coincidan y de que las configuraciones de destino de todos los subconjuntos que se están modificando son únicas.

Intercambiar instancias reservadas convertibles

Puede intercambiar una o varias instancias reservadas convertibles por otra instancia reservada convertible con una configuración diferente, incluida la familia de instancias, el sistema operativo y la tenencia. No hay ningún límite en cuanto al número de veces que puede hacer un intercambio, siempre que la nueva instancia reservada convertible tenga un valor igual o superior al de las instancias reservadas convertibles que está intercambiando.

Cuando se intercambia una instancia reservada convertible, la cantidad de instancias de la reserva actual se intercambia por la cantidad de instancias que cubre el valor igual o superior de la configuración de la nueva instancia reservada convertible. Amazon EC2 calcula la cantidad de instancias reservadas que puede recibir por el intercambio.

No se puede intercambiar estándar instancias reservadas, pero puede modificarlas. Para obtener más información, consulte Modificar instancias reservadas .

Contenido

Requisitos para el intercambio de instancias reservadas convertibles

Si se cumplen las siguientes condiciones, Amazon EC2 procesará su solicitud de intercambio. Su instancia reservada convertible debe estar:

- Activa
- No hay otra solicitud de intercambio pendiente.
- Tiene al menos 24 horas antes de que caduque

Se aplican las siguientes reglas:

- Las instancias reservadas convertibles solo se pueden intercambiar por otras instancias reservadas convertibles ofrecidas por AWS.
- Las instancias reservadas convertibles están asociadas con una región específica, que es fija mientras dure la reserva. No se puede intercambiar una instancia reservada convertible por una instancia reservada convertible de una región diferente.
- Puede intercambiar una o varias instancias reservadas convertibles a la vez para obtener una única instancia reservada convertible.
- Para intercambiar solo una parte de una instancia reservada convertible, puede modificarla y convertirla en dos o más reservas y después intercambiar una o varias de dichas reservas por otra instancia reservada convertible. Para obtener más información, consulte Intercambiar una parte de un instancia reservada convertible. Para obtener más información sobre cómo modificar instancias reservadas, consulte Modificar instancias reservadas.
- Todas las instancias reservadas convertibles de pago inicial total se pueden intercambiar por instancias reservadas convertibles de pago inicial parcial, y viceversa.

> **Note**
>
> Si el pago inicial total necesario para el intercambio (costo de nivelación) es inferior a 0,00 USD, AWS brinda automáticamente una cantidad de instancias en la instancia reservada convertible que garantiza que el costo de nivelación es como mínimo 0,00 USD.

> **Note**
>
> Si el valor total (precio inicial + precio por hora * cantidad de horas restantes) de la instancia reservada convertible nueva es inferior al valor total de la instancia reservada convertible intercambiada, AWS brinda automáticamente una cantidad de instancias en la instancia reservada convertible que garantiza que el valor total es mayor o igual que el de la instancia reservada convertible intercambiada.

- Para poder beneficiarse de mejores precios, puede intercambiar una instancia reservada convertible sin pagos iniciales por una instancia reservada convertible con pago inicial total o pago inicial parcial.
- No puede intercambiar las instancias reservadas convertibles con pago inicial total o pago inicial parcial por instancias reservadas convertibles sin pago inicial.

- Puede intercambiar una instancia reservada convertible sin pago inicial por otra instancia reservada convertible sin pago inicial solo si el precio por hora de la instancia reservada convertible nueva es mayor o igual que el de la instancia reservada convertible intercambiada.

  > **Note**
  >
  > Si el valor total (precio por hora * cantidad de horas restantes) de la instancia reservada convertible nueva es inferior al valor total de la instancia reservada convertible intercambiada, AWS brinda automáticamente una cantidad de instancias en la instancia reservada convertible que garantiza que el valor total es mayor o igual que el de la instancia reservada convertible intercambiada.

- Si intercambia varias instancias reservadas convertibles que tienen fechas de vencimiento diferentes, la fecha de vencimiento de la instancia reservada convertible nueva será la fecha más lejana en el futuro.
- Si intercambia una sola instancia reservada convertible, esta debe tener el mismo plazo (1 o 3 años) que la instancia reservada convertible nueva. Si fusiona varias instancias reservadas convertibles que tengan plazos diferentes, la instancia reservada convertible nueva tendrá un plazo de 3 años. Para obtener más información, consulte Fusionar instancias reservadas convertibles.
- Cuando Amazon EC2 intercambia una instancia reservada convertible, retira la reserva asociada y transfiere la fecha de finalización a la nueva reserva. Tras el intercambio, Amazon EC2 establece la fecha de finalización de la reserva anterior y la fecha de inicio de la nueva reserva igual a la fecha del cambio. Por ejemplo, si cancela una reserva de tres años a la que aún le quedaban 16 meses de plazo, la nueva reserva es de 16 meses con la misma fecha de finalización que la reserva de la instancia reservada convertible que ha intercambiado.

Calcular instancias reservadas convertibles intercambios

El intercambio de instancias reservadas convertibles es gratuito. No obstante, es posible que deba pagar un costo de nivelación, que es un costo inicial prorrateado de la diferencia entre las instancias reservadas convertibles que tenía y las nuevas instancias reservadas convertibles que recibe del intercambio.

Cada instancia reservada convertible tiene un valor de lista. Este valor de lista se compara con el valor de lista de las instancias reservadas convertibles que desea con el fin de determinar cuántas reservas de instancias puede recibir del intercambio.

Por ejemplo: tiene una instancia reservada convertible con un valor de lista de 35 USD que desea intercambiar por un tipo de instancia nuevo con un valor de lista de 10 USD.

```
$35/$10 = 3.5
```

Puede intercambiar la instancia reservada convertible por tres instancias reservadas convertibles de 10 USD. No se puede comprar media reserva, por lo que tendrá que comprar una instancia reservada convertible adicional que cubra el resto:

```
3.5 = 3 whole Convertible Reserved Instances + 1 additional Convertible Reserved
 Instance
```

La cuarta instancia reservada convertible tiene la misma fecha de finalización que las otras tres. Si está intercambiando instancias reservadas convertibles de pagos iniciales parciales o totales, deberá pagar el costo de nivelación de la cuarta reserva. Si el costo inicial restante de las instancias reservadas convertibles es de 500 USD y la nueva reserva normalmente costaría 600 USD en forma prorrateada, se le cobrarán 100 USD.

```
$600 prorated upfront cost of new reservations - $500 remaining upfront cost of old
 reservations = $100 difference
```

Fusionar instancias reservadas convertibles

Si fusiona dos o más instancias reservadas convertibles, el plazo de la instancia reservada convertible nueva tiene que ser el mismo que el de las instancias reservadas convertibles originales o el que venza más tarde de las instancias reservadas convertibles. La fecha de vencimiento de la nueva instancia reservada convertible será la fecha más lejana en el futuro.

Suponga, por ejemplo, que tenga las instancias reservadas convertibles siguientes en su cuenta:

ID de instancia reservada	Plazo	Fecha de vencimiento
aaaa1111	1 año	31/12/2018
bbbb2222	1 año	31/07/2018
cccc3333	3 años	30/06/2018
dddd4444	3 años	31/12/2019

- Puede fusionar `aaaa1111` y `bbbb2222` e intercambiarlas por una instancia reservada convertible de un año. No puede intercambiarlos por una instancia reservada convertible de tres años. La fecha de vencimiento de la nueva instancia reservada convertible es el 31/12/2018.
- Puede fusionar `bbbb2222` y `cccc3333` e intercambiarlas por una instancia reservada convertible de 3 años. No puede intercambiarlos por una instancia reservada convertible de un año. La fecha de vencimiento de la nueva instancia reservada convertible es el 31/07/2018.
- Puede fusionar `cccc3333` y `dddd4444` e intercambiarlas por una instancia reservada convertible de 3 años. No puede intercambiarlos por una instancia reservada convertible de un año. La fecha de vencimiento de la nueva instancia reservada convertible es el 31/12/2019.

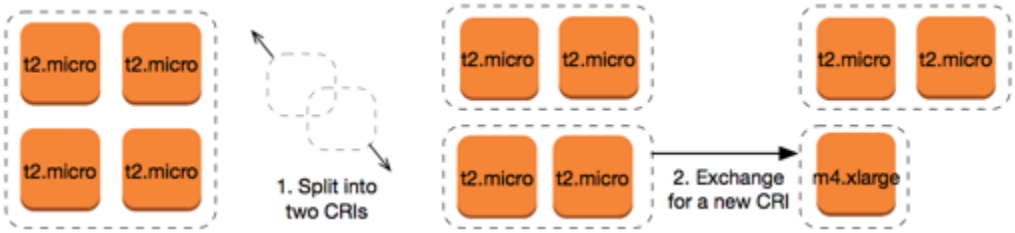
Intercambiar una parte de un instancia reservada convertible

Puede utilizar el proceso de modificación para dividir la instancia reservada convertible en reservas más pequeñas y después intercambiar una o varias de dichas reservas por otra instancia reservada convertible. En los siguientes ejemplos se muestra cómo realizar esta operación.

Example Ejemplo; instancia reservada convertible con varias instancias

En este ejemplo, tiene una instancia reservada convertible `t2.micro` con cuatro instancias en la reserva. Para intercambiar dos instancias `t2.micro` por una instancia `m4.xlarge`:

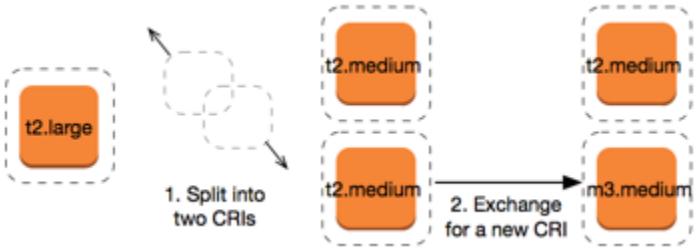
1. Modifique la instancia reservada convertible `t2.micro` dividiéndola en dos instancias reservadas convertibles `t2.micro` con dos instancias cada una.
2. Intercambie una de las `t2.micro` instancias reservadas convertibles nuevas por una instancia reservada convertible `m4.xlarge`.



Example Ejemplo; instancia reservada convertible con una instancia

En este ejemplo, tiene una instancia reservada convertible `t2.large`. Para cambiarla por una instancia `t2.medium` más pequeña y una instancia `m3.medium`:

1. Modifique la instancia reservada convertible `t2.large` dividiéndola en dos instancias reservadas convertibles `t2.medium`. Una única instancia `t2.large` tiene el mismo tamaño de instancia que dos instancias `t2.medium`.
2. Intercambie una de las instancias reservadas convertibles `t2.medium` nuevas por una instancia reservada convertible `m3.medium`.



Para obtener más información, consulte Compatibilidad para modificar tamaños de instancia y Enviar solicitudes de intercambio.

Enviar solicitudes de intercambio

Puede intercambiar las instancias reservadas convertibles utilizando la consola de Amazon EC2 o una herramienta de línea de comandos.

Intercambiar una instancia reservada convertible mediante la consola

Puede buscar ofertas de instancias reservadas convertibles y seleccionar la nueva configuración entre las opciones ofrecidas.

New console

Cómo intercambiar instancias reservadas convertibles mediante la consola de Amazon EC2

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. Elija Reserved Instances (instancias reservadas), seleccione las instancias reservadas convertibles que desea intercambiar y elija Actions (Acciones), Exchange instancia reservada (Intercambiar la instancia reservada).
3. Seleccione los atributos de la configuración deseada y elija Find offering (Buscar oferta).
4. Seleccione una nueva instancia reservada convertible. En la parte inferior de la pantalla, puede ver el número de instancias reservadas que recibe para el intercambio y cualquier costo adicional.

5. Cuando haya seleccionado una instancia reservada convertible que cumpla sus necesidades, elija Review (Revisar).
6. Elija Exchange (Intercambiar) y, a continuación, Close (Cerrar).

Old console

Cómo intercambiar instancias reservadas convertibles mediante la consola de Amazon EC2

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. Elija Reserved Instances (instancias reservadas), seleccione las instancias reservadas convertibles que desea intercambiar y elija Actions (Acciones), Exchange instancia reservada (Intercambiar la instancia reservada).
3. Seleccione los atributos de la configuración deseada y elija Find Offering (Buscar oferta).
4. Seleccione una nueva instancia reservada convertible. La columna Instance Count (Recuento de instancias) muestra el número de instancias reservadas que recibe por el intercambio. Cuando haya seleccionado una instancia reservada convertible que cumpla sus necesidades, elija Exchange (Intercambiar).

Las instancias reservadas que se han intercambiado se retiran y las instancias reservadas nuevas se muestran en la consola de Amazon EC2. Este proceso puede tardar unos minutos en propagarse.

Intercambiar una instancia reservada convertible con la interfaz de línea de comandos

Para intercambiar una instancia reservada convertible, primero encuentre una nueva instancia reservada convertible que cumpla sus necesidades:

- describe-reserved-instances-offerings (AWS CLI)
- Get-EC2ReservedInstancesOffering (Herramientas para Windows PowerShell)

Obtenga un presupuesto para el intercambio que incluya el número de instancias reservadas que conseguirá en el intercambio y el verdadero costo de nivelación del intercambio:

- get-reserved-instances-exchange-quote (AWS CLI)
- GetEC2-ReservedInstancesExchangeQuote (Herramientas para Windows PowerShell)

Finalmente, lleve a cabo el intercambio.

- accept-reserved-instances-exchange-quote (AWS CLI)
- Confirm-EC2ReservedInstancesExchangeQuote (Herramientas para Windows PowerShell)

Cuotas de instancia reservada

Puede comprar nuevas instancias reservadas todos los meses. El número de instancias reservadas nuevas que puede comprar al mes se determina según la cuota mensual, como se detalla a continuación:

Descripción de la cuota	Cuota predeterminada
instancias reservadas regionales nuevas	20 por región al mes
instancias reservadas de zona nuevas	20 por zona de disponibilidad al mes

Por ejemplo, en una región con tres zonas de disponibilidad, la cuota predeterminada es de 80 instancias reservadas nuevas al mes y se calcula de la siguiente forma:

- 20 instancias reservadas regionales para la región
- Más 60 instancias reservadas de zona (20 para cada una de las tres zonas de disponibilidad)

Las instancias con el estado `running` se tienen en cuenta para la cuota. Las instancias con los estados `pending`, `stopping`, `stopped` y `hibernated` no se tienen en cuenta para la cuota.

Visualización del número de instancias reservadas compradas

El número de instancias reservadas que compre se indica en el campo Instance count (Recuento de instancias) de la consola o mediante el parámetro `InstanceCount` en la AWS CLI. Cuando compra nuevas instancias reservadas, la cuota se mide en relación con el recuento total de instancias. Por ejemplo, si compra una configuración de instancia reservada única con un recuento de 10 instancias, la compra se cuenta en relación con la cuota como 10, no como 1.

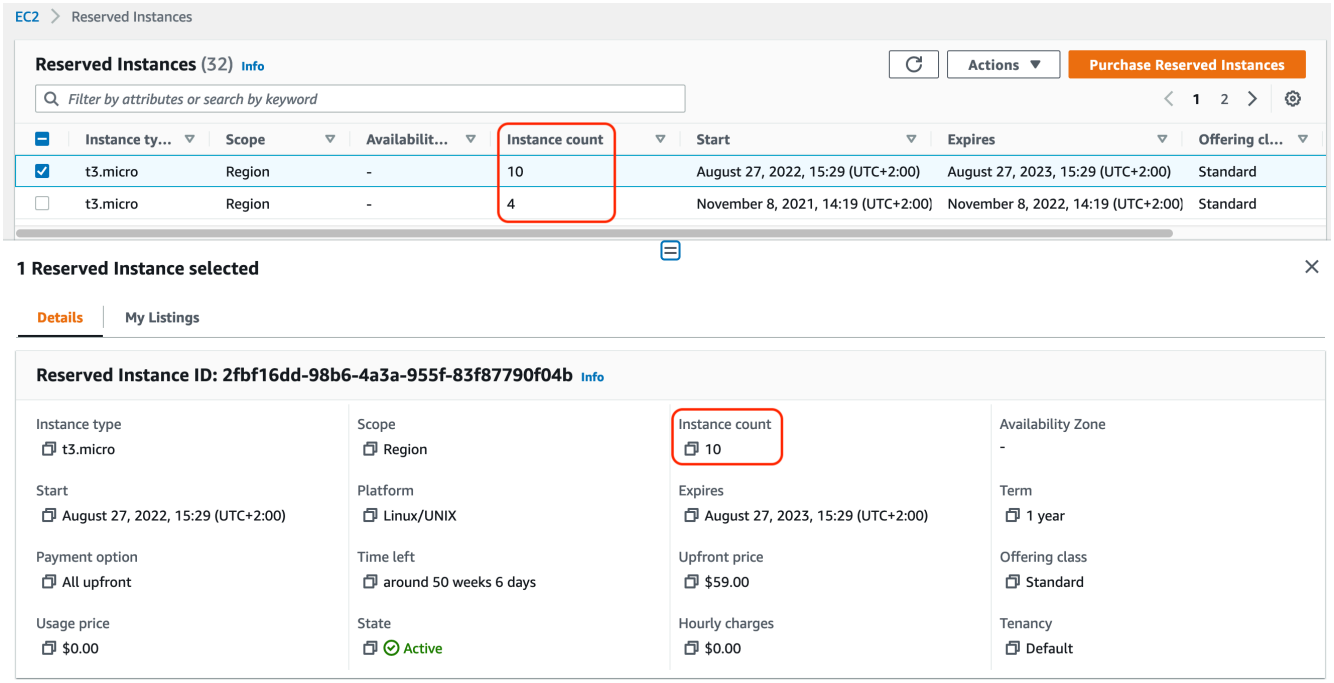
Puede ver el número de instancias reservadas que ha comprado mediante Amazon EC2 o la AWS CLI.

Console

Visualización del número de instancias reservadas compradas

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Reserved Instances (instancias reservadas).
3. Seleccione una configuración de instancia reservada de la tabla y compruebe el campo Instance count (Recuento de instancias).

   En la siguiente captura de pantalla, la línea seleccionada representa una configuración de instancia reservada única para un tipo de instancia `t3.micro`. La columna Instance count (Recuento de instancias) de la vista de tabla y el campo Instance count (Recuento de instancias) de la vista de detalles (que se marcan en la captura de pantalla) indican que hay 10 instancias reservadas para esta configuración.



AWS CLI

Visualización del número de instancias reservadas compradas

Utilice el comando de la CLI describe-reserved-instances y especifique el ID de la configuración de instancia reservada.

```
aws ec2 describe-reserved-instances \
```

```
    --reserved-instances-ids 2fbf16dd-98b6-4a3a-955f-83f87790f04b \
    --output table
```

Ejemplo de salida: el campo `InstanceCount` indica que hay 10 instancias reservadas para esta configuración.

```
-------------------------------------------------------------------
|                   DescribeReservedInstances                     |
+-----------------------------------------------------------------+
||                       ReservedInstances                       ||
|+----------------------+----------------------------------------+|
||  CurrencyCode        |  USD                                   ||
||  Duration            |  31536000                              ||
||  End                 |  2023-08-27T13:29:44+00:00             ||
||  FixedPrice          |  59.0                                  ||
||  InstanceCount       |  10                                    ||
||  InstanceTenancy     |  default                               ||
||  InstanceType        |  t3.micro                              ||
||  OfferingClass       |  standard                              ||
||  OfferingType        |  All Upfront                           ||
||  ProductDescription  |  Linux/UNIX                            ||
||  ReservedInstancesId |  2fbf16dd-98b6-4a3a-955f-83f87790f04b  ||
||  Scope               |  Region                                ||
||  Start               |  2022-08-27T13:29:45.938000+00:00      ||
||  State               |  active                                ||
||  UsagePrice          |  0.0                                   ||
|+----------------------+----------------------------------------+|
|||                      RecurringCharges                       |||
||+---------------------------------+--------------------------+||
|||  Amount                         |  0.0                     |||
|||  Frequency                      |  Hourly                  |||
||+---------------------------------+--------------------------+||
```

Consideraciones

Una instancia reservada regional aplica un descuento a una instancia a petición en ejecución. El límite predeterminado de instancia a petición es de 20. No puede superar el límite de instancia a petición en ejecución adquiriendo instancias reservadas regionales. Por ejemplo, si ya tiene 20 instancias bajo demanda en ejecución y adquiere 20 instancias reservadas regionales, estas 20 instancias reservadas regionales se utilizan para aplicar un descuento a las 20 instancias bajo

demanda en ejecución. Si adquiere más instancias reservadas regionales, no podrá iniciar más instancias debido a que habrá alcanzado el límite de instancia a petición.

Antes de adquirir instancias reservadas regionales, asegúrese de que su límite de instancia a petición coincide o supera el número de instancias reservadas regionales que quiere poseer. Si es necesario, asegúrese de solicitar un incremento del límite de instancia a petición antes de adquirir más instancias reservadas regionales.

Una instancia reservada de zona, es decir, una instancia reservada que se adquiere para una zona de disponibilidad específica, proporciona una reserva de capacidad, así como un descuento. Puede superar el límite de instancia a petición en ejecución adquiriendo instancias reservadas zonales. Por ejemplo, si ya tiene 20 instancias bajo demanda en ejecución y adquiere 20 instancias reservadas zonales, puede iniciar 20 instancias bajo demanda adicionales que coincidan con las especificaciones de las instancias reservadas zonales, lo que suma un total de 40 instancias en ejecución.

Visualización de cuotas de instancia reservada y solicitud de un aumento de cuota

La consola de Amazon EC2 proporciona información sobre las cuotas. También puede solicitar un aumento de cuotas. Para obtener más información, consulte Visualización de las cuotas actuales y Solicitar un aumento.

Spot Instances

Una instancia de spot es una instancia que utiliza la capacidad sobrante de EC2 que está disponible por un precio inferior con respecto al precio bajo demanda. Dado que las instancias de spot permiten solicitar instancias de EC2 no utilizadas con grandes descuentos, es posible reducir considerablemente los costos de Amazon EC2. El precio por hora de una instancia de spot se denomina precio de spot. Amazon EC2 establece el precio de spot de cada tipo de instancia en cada zona de disponibilidad, y este fluctúa en función de la oferta y la demanda a largo plazo de las instancias de spot. La instancia de spot se ejecuta siempre que haya capacidad disponible.

Las instancias de spot son una opción económica si es flexible con respecto a cuándo es necesario ejecutar las aplicaciones y si las aplicaciones se pueden interrumpir. Por ejemplo, las instancias de spot son adecuadas para análisis de datos, trabajos por lotes, procesamiento en segundo plano y tareas opcionales. Para obtener más información, consulte Precios de instancias de spot de Amazon EC2.

Para comparar las distintas opciones de compra de instancias de EC2, consulte Opciones de compra de instancias.

Temas

Conceptos

Antes de comenzar con las instancias de spot, familiarícese con los siguientes conceptos:

- Grupo de capacidad de spot: un conjunto de instancias de EC2 no utilizadas con el mismo tipo de instancia (por ejemplo: `m5.large`) y zona de disponibilidad.
- Precio de spot: el precio actual de una instancia de spot por hora.
- Solicitud de instancia de Spot: Solicita una instancia de spot. Cuando hay capacidad disponible, Amazon EC2 satisface su solicitud. Una solicitud de instancia de spot es única o persistente. Amazon EC2 vuelve a enviar de forma automática una solicitud de instancia de spot persistente en cuanto se interrumpe la instancia de spot asociada a la solicitud.

- Recomendación de reequilibrio de instancias de EC2: Amazon EC2 emite una señal de recomendación de reequilibrio de instancia para notificarle que la instancia de spot tiene un riesgo elevado de interrupción. Esta señal brinda la oportunidad de reequilibrar proactivamente sus cargas de trabajo entre las instancias de spot existentes o nuevas sin tener que esperar el aviso de interrupción de la instancia de spot con dos minutos de anticipación.
- Interrupción de instancia de spot: Amazon EC2 termina, detiene o hiberna la instancia de spot cuando Amazon EC2 necesita de nuevo la capacidad. Amazon EC2 envía un aviso de interrupción de la instancia de spot, que otorga a la instancia una advertencia dos minutos antes de que se interrumpa.

Diferencias clave entre instancias de spot y instancias bajo demanda

En la siguiente tabla, se muestran las principales diferencias entre las instancias de spot y las instancias bajo demanda.

	Spot Instances	On-Demand Instances
Hora de inicialización	Solo se pueden iniciar inmediatamente si la solicitud de instancia de spot está activa y hay capacidad disponible.	Solo se pueden iniciar inmediata mente si se realiza una solicitud de inicialización manual y hay capacidad disponible.
Capacidad disponible	Si no hay capacidad disponible, la solicitud de instancia de spot sigue realizando la solicitud de inicialización de manera automática hasta que se disponga de capacidad.	Si no hay capacidad disponible al realizar una solicitud de inicialización, recibirá un error de capacidad insuficie nte (ICE).
Precio por hora	El precio por hora de las instancias de spot varía en función del suministro y la demanda a largo plazo.	El precio por hora de las instancias bajo demanda es estático.
Recomenda ción de reequilibrio	La señal que emite Amazon EC2 para una instancia de spot en ejecución	Determine cuándo se interrumpe una instancia a petición (se detiene, se hiberna o se termina).

	Spot Instances	On-Demand Instances
	cuando la instancia tiene un riesgo elevado de interrupción.	
Interrupción de instancias	Puede detener e iniciar una instancia de spot con respaldo de Amazon EBS. Además, Amazon EC2 puede interrumpir una instancia de spot individual si la capacidad ya no está disponible.	Determine cuándo se interrumpe una instancia a petición (se detiene, se hiberna o se termina).

Cómo comenzar

Lo primero que tiene que hacer es prepararse para usar Amazon EC2. También puede resultarle de utilidad tener experiencia en la inicialización de instancias bajo demanda antes de iniciar instancias de spot.

Conceptos básicos de las spot

- Cómo funcionan las instancias de spot

Uso de instancias de spot

- Crear una solicitud de instancia de spot
- Obtener información del estado de la solicitud
- Interrupciones de instancias de spot

Servicios relacionados

Puede aprovisionar instancias de spot directamente mediante Amazon EC2. También puede aprovisionar instancias de spot con otros servicios de AWS. Para obtener más información, consulte la documentación siguiente.

Amazon EC2 Auto Scaling e instancias de spot

Puede crear configuraciones o plantillas de inicialización para que Amazon EC2 Auto Scaling pueda iniciar instancias de spot. Para obtener más información, consulte Solicitud de instancias

de spot para aplicaciones flexibles y tolerantes a fallos y Grupos de escalado automático con varios tipos de instancias y opciones de compra en la Guía del usuario de Amazon EC2 Auto Scaling.

Amazon EMR y instancias de spot

Existen situaciones en las que puede resultar útil ejecutar instancias de spot en un clúster de Amazon EMR. Para obtener más información, consulte instancias de spot y ¿Cuándo se deben utilizar las instancias de spot? en la Guía de administración de Amazon EMR.

AWS CloudFormationPlantillas de

AWS CloudFormation permite crear y administrar una colección de recursos de AWS mediante una plantilla en formato JSON. Para obtener más información, consulte Actualizaciones de instancias de spot EC2: Spot - escalado automático e integración de CloudFormation.

AWS SDK for Java

Se puede usar el lenguaje de programación Java para administrar las instancias de spot. Para obtener más información, consulte Tutorial: instancias de spot de Amazon EC2 y Tutorial: Administración avanzada de solicitudes de spot de Amazon EC2.

AWS SDK for .NET

Se puede usar el entorno de programación .NET para administrar las instancias de spot. Para obtener más información, consulte Tutorial: instancias de spot de Amazon EC2.

Precios y ahorro

Las instancias de spot se cobran según el precio de spot, establecido por Amazon EC2. Este precio se ajusta gradualmente en función de la oferta y la demanda a largo plazo de las instancias de spot. Las instancias de spot se ejecutan hasta que las termina, hasta que no haya capacidad disponible o hasta que su grupo de Amazon EC2 Auto Scaling las termine durante la reducción horizontal.

Si usted o Amazon EC2 interrumpe una instancia de spot en ejecución, se le cobrará por los segundos utilizados o por la hora completa, o no se le aplicará ningún cargo, en función del sistema operativo que utilice y de quién interrumpió la instancia de spot. Para obtener más información, consulte Facturación de las instancias de spot interrumpidas.

Savings Plans no cubre las instancias de spot. Si cuenta con un Savings Plan, este no ofrece ahorros adicionales a los que ya obtiene al utilizar las instancias de spot. Además, los gastos en las instancias de spot no se aplican a los compromisos de los Savings Plans para computación.

Ver precios

Para ver el precio actual más bajo de spot (actualizado cada cinco minutos) por Región de AWS y tipo de instancia, consulte la página Precios de instancias de spot de Amazon EC2.

Para ver el historial de precios de spot de los últimos tres meses, utilice la consola de Amazon EC2 o el comando Describir historial de precios de spot (AWS CLI). Para obtener más información, consulte Historial de precios de instancias de spot.

De forma independiente, asignamos zonas de disponibilidad a códigos para cada Cuenta de AWS. Por ese motivo, puede obtener diferentes resultados para el mismo código de zona de disponibilidad (por ejemplo, `us-west-2a`) entre diferentes cuentas.

Ver el ahorro

Puede ver los ahorros obtenidos mediante el uso de instancias de spot para una sola flota de spot o para todas las instancias de spot. Puede ver el ahorro conseguido durante la última hora o los últimos tres días y el precio medio por hora de CPU virtual y por hora de memoria (GiB). El ahorro es una estimación y podría diferir del ahorro real porque no incluye los ajustes en la facturación en función del uso. Para obtener más información acerca de la visualización de información sobre el ahorro, consulte Ahorro en la compra de instancias de spot.

Ver facturación

Su factura proporciona detalles sobre el uso del servicio. Para obtener más información, consulte Ver su factura en la Guía del usuario de AWS Billing.

Prácticas recomendadas para instancias de spot de EC2

Las instancias de spot de Amazon EC2 son capacidades de cómputo de EC2 de reserva en Nube de AWS, que están disponibles con un ahorro de hasta un 90 % de descuento en comparación con los precios bajo demanda. La única diferencia entre instancias bajo demanda y instancias de spot es que Amazon EC2 puede interrumpir las instancias de spot, con dos minutos de notificación, cuando Amazon EC2 necesita de nuevo la capacidad.

Se recomienda el uso de instancias de spot para aplicaciones sin estado, tolerantes a fallos y flexibles. Por ejemplo, las instancias de spot funciona bien para big data, cargas de trabajo en contenedores, CI/CD, servidores web sin estado, informática de alto rendimiento (HPC) y cargas de trabajo de representación.

Mientras se ejecutan, las instancias de spot son exactamente iguales que las instancias bajo demanda. Sin embargo, las instancias de spot no garantizan que pueda mantener las instancias en ejecución el tiempo suficiente para finalizar sus cargas de trabajo. Las instancias de spot tampoco garantizan que pueda obtener disponibilidad inmediata de las instancias que está buscando, ni que siempre pueda obtener la capacidad agregada que solicitó. Además, las interrupciones y la capacidad de las instancias de spot pueden cambiar con el paso del tiempo porque la disponibilidad de instancias de spot varía según la oferta y la demanda, y el rendimiento pasado no es garantía de resultados futuros.

Las instancias de spot no son adecuadas para cargas de trabajo que no sean flexibles, con estado, sin tolerancia a errores o estrechamente acopladas entre nodos de instancia. No se recomienda utilizar instancias de spot para las cargas de trabajo que no sean tolerantes a periodos ocasionales en los que la capacidad de destino en su totalidad no esté completamente disponible. Si bien seguir las prácticas recomendadas de spot para ser flexible en cuanto a los tipos de instancias y las zonas de disponibilidad es la mejor opción para obtener una alta disponibilidad, no hay garantías de que la capacidad esté disponible, ya que el aumento de la demanda de instancias bajo demanda puede interrumpir las cargas de trabajo en las instancias de spot.

Es de suma importancia que no se utilicen instancias de spot para estas cargas de trabajo ni que se intente realizar una conmutación por error a instancias bajo demanda para controlar las interrupciones o los periodos de falta de disponibilidad. La conmutación por error de instancias bajo demanda puede provocar interrupciones inadvertidas en el resto de las instancias de spot. Además, si se interrumpen las instancias de spot de una combinación de una instancia y una zona de disponibilidad, puede resultar difícil conseguir instancias bajo demanda con la misma combinación.

Con independencia de si es un usuario de instancias de spot con experiencia o no conoce este tipo de instancias, si está experimentando problemas con interrupciones o disponibilidad de instancias de spot, le aconsejamos que siga estas prácticas recomendadas para tener la mejor experiencia con el servicio de instancias de spot.

Prácticas recomendadas para instancias de spot

- Preparar instancias individuales para interrupciones
- Sea flexible con respecto a los tipos de instancia y las zonas de disponibilidad
- Uso de grupos de escalado automático de EC2 o flota de EC2 para administrar la capacidad agrupada
- Utilice la estrategia de asignación optimizada para capacidad y precio
- Utilice servicios integrados de AWS para administrar sus instancias de spot

- ¿Cuál es el mejor método de solicitud de spot que se puede utilizar?

Preparar instancias individuales para interrupciones

La mejor manera de gestionar las interrupciones de instancias de spot correctamente es diseñar su aplicación para que sea tolerante a errores. Para lograrlo, puede aprovechar las recomendaciones de reequilibrio de instancia de EC2 y los avisos de interrupción de instancias de spot.

Una recomendación de reequilibrio de instancia de EC2 es una señal que notifica cuando una instancia de spot corre un riesgo elevado de interrupción. La señal brinda la oportunidad de administrar la instancia de spot de forma proactiva antes del aviso de interrupción de instancia de spot de dos minutos de anticipación. Puede decidir reequilibrar su carga de trabajo con instancias de spot nuevos o existentes que no tengan un riesgo elevado de interrupción. Hemos facilitado el uso de esta señal mediante la característica de reequilibrio de capacidad en los grupos de escalado automático y flota de EC2.

Un aviso de interrupción de instancia de spot es una advertencia que se emite dos minutos antes de que Amazon EC2 interrumpa una instancia de spot. Si su carga de trabajo acepta “cambios de programación”, puede configurar sus instancias de spot para que se detengan o hibernen, en lugar de terminarlas, cuando se interrumpan. Amazon EC2 detiene o hiberna automáticamente sus instancias de spot en caso de interrupción y las reanuda también de manera automática cuando hay capacidad disponible.

Se recomienda crear una regla en Amazon EventBridge que capture las recomendaciones de reequilibrio y las notificaciones de interrupción y, a continuación, active un punto de control para el progreso de la carga de trabajo o gestione correctamente la interrupción. Para obtener más información, consulte Monitorear las señales de recomendación de reequilibrio. Para obtener un ejemplo detallado que le explica cómo crear y utilizar reglas de eventos, consulte Aprovechamiento de los avisos de interrupción de instancias de spot de Amazon EC2.

Para obtener más información, consulte Recomendación de reequilibrio de instancias de EC2 y Interrupciones de instancias de spot.

Sea flexible con respecto a los tipos de instancia y las zonas de disponibilidad

Un grupo de capacidad de spot es un conjunto de instancias de EC2 que no se utilizan con el mismo tipo de instancia (por ejemplo, `m5.large`) y zona de disponibilidad (por ejemplo: us-east-1a). Debe ser flexible en cuanto a los tipos de instancia que solicita y las zonas de disponibilidad en las que puede implementar la carga de trabajo. Esto le da a las instancias de spot una mejor oportunidad

de encontrar y asignar la cantidad necesaria de capacidad de cómputo. Por ejemplo, no pida solo `c5.large` si estaría dispuesto a usar larges de las familias c4, m5 y m4.

En función de sus necesidades concretas, puede evaluar con qué tipos de instancia puede ser flexible para cumplir sus requisitos informáticos. Si una carga de trabajo se puede escalar verticalmente, debe incluir tipos de instancia más grandes (más vCPU y memoria) en sus solicitudes. Si solo puede escalar horizontalmente, debe incluir tipos de instancias de generación anterior, ya que tienen menos demanda de los clientes bajo demanda.

Una buena regla general es ser flexible con al menos 10 tipos de instancias para cada carga de trabajo. Además, asegúrese de que todas las zonas de disponibilidad estén configuradas para su uso en la VPC y seleccionadas para su carga de trabajo.

Uso de grupos de escalado automático de EC2 o flota de EC2 para administrar la capacidad agrupada

Las instancias de spot le permiten pensar en términos de capacidad agrupada, en unidades que incluyen vCPU, memoria, almacenamiento o rendimiento de red, en lugar de pensar en términos de instancias individuales. Los grupos de escalado automático y flota de EC2 le permiten iniciar y mantener una capacidad de destino, así como solicitar automáticamente recursos para reemplazar cualquier recurso que sufra una interrupción o terminación manual. Cuando configura un grupo de escalado automático o una flota de EC2, solo tiene que especificar los tipos de instancia y la capacidad de destino en función de las necesidades de la aplicación. Para obtener más información, consulte Grupos de escalado automático en la Guía del usuario de Amazon EC2 Auto Scaling y Crear una flota de EC2 en esta guía del usuario.

Utilice la estrategia de asignación optimizada para capacidad y precio

Las estrategias de asignación en grupos de Auto Scaling ayudan a aprovisionar la capacidad de destino sin necesidad de buscar manualmente los grupos de capacidad de spot con capacidad sobrante. Recomendamos utilizar la estrategia `price-capacity-optimized` porque aprovisiona automáticamente instancias de los grupos de capacidad de spot más disponibles que también tienen el precio más bajo posible. También puede usar la estrategia de asignación `price-capacity-optimized` en flota de EC2. Debido a que la capacidad de la instancia de spot proviene de grupos con capacidad óptima, esto disminuye la posibilidad de que se reclamen las instancias de spot. Para obtener más información acerca de las estrategias de asignación, consulte instancias de spot en Guía del usuario de Amazon EC2 Auto Scaling y Cuando las cargas de trabajo tienen un alto costo de interrupción en esta guía del usuario.

Utilice servicios integrados de AWS para administrar sus instancias de spot

Otros servicios de AWS se integran con instancias de spot para reducir los costos informáticos generales sin necesidad de administrar las instancias o flotas individuales. Le recomendamos que se plantee utilizar las siguientes soluciones para sus cargas de trabajo aplicables: Amazon EMR, Amazon Elastic Container Service, AWS Batch, Amazon Elastic Kubernetes Service, Amazon SageMaker, AWS Elastic Beanstalk y Amazon GameLift. Para obtener más información sobre las prácticas recomendadas de instancias de spot con estos servicios, consulte el sitio web de Amazon EC2 instancias de spot Workshops.

¿Cuál es el mejor método de solicitud de spot que se puede utilizar?

Use la siguiente tabla para determinar qué API debe utilizar al solicitar instancias de spot.

API	¿Cuándo se debe utilizar?	Caso de uso	¿Debo utilizar esta API?
CreateAutoScalingGroup	• Necesita varias instancias con una configuración única o una configuración mixta. • Desea automatizar la administración del ciclo de vida mediante una API configurable.	Cree un grupo de Auto Scaling que administre el ciclo de vida de las instancias a la vez que mantiene el número de instancias deseado. Admite escalado horizontal (agregar más instancias) entre los límites mínimo y máximo especificados.	Sí
CreateFleet	• Necesita varias instancias con una configuración única o una configuración mixta.	Cree una flota de instancias bajo demanda e instancias de spot en una única solicitud, con varias especificaciones de	Sí, en modo `instant` si no necesita escalado automático

API	¿Cuándo se debe utilizar?	Caso de uso	¿Debo utilizar esta API?
	• Desea administrar por sí mismo el ciclo de vida de las instancias. • Si no necesita escalado automático, se recomienda utilizar el tipo de flota `instant`.	inicialización que varían por tipo de instancia, AMI, zona de disponibilidad o subred. La estrategia de asignación de instancias de spot se establece de manera predeterminada como `lowest-price` por unidad, pero se puede cambiar a `price-capacity-optimized` , `capacity-optimized` o `diversified` .	

API	¿Cuándo se debe utilizar?	Caso de uso	¿Debo utilizar esta API?
RunInstances	• Ya está utilizando la API RunInstances para iniciar instancias bajo demanda, y simplemente desea cambiar a iniciar instancias de spot modificando un único parámetro. • No necesita varias instancias con distintos tipos de instancias.	Lance un número especificado de instancias utilizando una AMI y un tipo de instancia.	No, porque RunInstances no permite tipos de instancias mixtos en una sola solicitud

API	¿Cuándo se debe utilizar?	Caso de uso	¿Debo utilizar esta API?
RequestSpotFleet	• Se desaconseja encarecidamente utilizar la API RequestSpotFleet, porque es una API heredada sin inversión planificada. • Si desea administrar el ciclo de vida de las instancias, utilice la API CreateFleet. • Si no desea administrar el ciclo de vida de las instancias, utilice la API CreateAutoScalingGroup.	NO UTILIZAR. RequestSpotFleet es una API heredada sin inversión planificada.	No
RequestSpotInstances	• Se desaconseja encarecidamente utilizar la API RequestSpotInstances, porque es una API heredada sin inversión planificada.	NO UTILIZAR. RequestSpotInstances es una API heredada sin inversión planificada.	No

Cómo funcionan las instancias de spot

Para iniciar una instancia de spot, puede crear una Solicitud de instancia de Spot, o Amazon EC2 crea una solicitud de instancia de spot en su nombre. La instancia de spot se inicia cuando se cumple la solicitud de instancia de spot.

Puede iniciar una instancia de spot usando varios servicios diferentes. Para obtener más información, consulte Introducción a las instancias de spot de Amazon EC2. En esta guía del usuario, describimos las siguientes formas de iniciar una instancia de spot usando EC2:

- Puede crear una solicitud de instancia de spot mediante el asistente de inicialización de instancias en la consola de Amazon EC2 o el comando de la AWS CLI run-instances. Para obtener más información, consulte Crear una solicitud de instancia de spot.
- Puede crear una flota de EC2, en la que especifique la cantidad deseada de instancias de spot. Amazon EC2 crea una solicitud de instancia de spot en su nombre para cada instancia de spot especificada en la flota de EC2. Para obtener más información, consulte Crear una flota de EC2.
- Puede crear una solicitud de flota de spot en la que especifique la cantidad deseada de instancias de spot. Amazon EC2 crea una solicitud de instancia de spot en su nombre para cada instancia de spot especificada en la solicitud de flota de spot. Para obtener más información, consulte Creación de una solicitud de flota de spot.

La instancia de spot se inicia si hay capacidad disponible.

La instancia de spot se ejecuta hasta que la detenga o la termine, o hasta que Amazon EC2 la interrumpa (lo que se conoce como una interrupción de instancia de spot).

Cuando utilice instancias de spot, debe estar preparado para las interrupciones. Amazon EC2 puede interrumpir su instancia de spot si la demanda de instancias de spot aumenta, si la oferta de instancias de spot disminuye. Cuando Amazon EC2 interrumpe una instancia de spot, proporciona un aviso de interrupción de instancia de spot, que envía a la instancia una advertencia dos minutos antes de que Amazon EC2 la interrumpa. No puede habilitar la protección contra terminación para instancias de spot. Para obtener más información, consulte Interrupciones de instancias de spot.

Puede detener, iniciar, reiniciar o terminar una instancia de spot con respaldo de Amazon EBS. El servicio de spot puede detener, terminar o hibernar una instancia de spot cuando la interrumpe.

Contenido

- iniciar instancias de spot en un grupo de zona de disponibilidad
- iniciar instancias de spot en una VPC

iniciar instancias de spot en un grupo de inicialización

Especifique un grupo de inicialización en la solicitud de instancia de spot para indicar a Amazon EC2 que lance un conjunto de instancias de spot solo si puede iniciarlas todas. Además, si el servicio de spot debe terminar una de las instancias de un grupo de inicialización, debe terminarlas todas. No obstante, si usted es el que termina una o más de las instancias en un grupo de inicialización, Amazon EC2 no termina el resto de las instancias del grupo de inicialización.

Si bien esta opción puede resultar útil, agregar esta limitación puede reducir las posibilidades de que se cumpla la solicitud de instancia de spot y aumentar las posibilidades de que se terminen las instancias de spot. Por ejemplo, el grupo de inicialización incluye instancias de múltiples zonas de disponibilidad. Si la capacidad de una de estas zonas de disponibilidad se reduce y ya no está disponible, entonces Amazon EC2 termina todas las instancias del grupo de inicialización.

Si crea otra solicitud de instancia de spot realizada correctamente que especifica el mismo grupo de inicialización (existente) que una solicitud anterior realizada correctamente, las instancias nuevas se agregarán al grupo de inicialización. Posteriormente, si se termina una instancia de este grupo de inicialización, se terminan todas las instancias del grupo, incluidas las instancias iniciadas en la primera y segunda solicitud.

iniciar instancias de spot en un grupo de zona de disponibilidad

Especifique un grupo de zona de disponibilidad en su solicitud de instancia de spot para indicar a Amazon EC2 que debe iniciar un conjunto de instancias de spot en la misma zona de disponibilidad. Amazon EC2 no necesita interrumpir todas las instancias de un grupo de zona de disponibilidad al mismo tiempo. Si Amazon EC2 debe interrumpir una de las instancias de un grupo de zona de disponibilidad, las demás siguen ejecutándose.

Si bien esta opción puede resultar útil, agregar esta limitación puede reducir las probabilidades de que se cumpla su solicitud de instancia de spot.

Si especifica un grupo de zona de disponibilidad, pero no una zona de disponibilidad en la solicitud de instancia de spot, el resultado dependerá de la red especificada.

VPC predeterminada

Amazon EC2 usa la zona de disponibilidad para la subred especificada. Si no especifica una subred, selecciona una zona de disponibilidad y su subred predeterminada, pero no necesariamente la zona más barata. Si eliminó la subred predeterminada para una zona de disponibilidad, entonces deberá especificar una subred diferente.

VPC no predeterminada

Amazon EC2 usa la zona de disponibilidad para la subred especificada.

iniciar instancias de spot en una VPC

La subred de las instancias de spot se especifica de la misma forma que una subred para las instancias bajo demanda.

- [VPC predeterminada] Si desea que la instancia de spot se lance en una zona de disponibilidad de bajo precio específica, debe especificar la subred correspondiente en la solicitud de instancia de spot. Si no especifica una subred, Amazon EC2 selecciona una automáticamente y la zona de disponibilidad de esta subred podría no tener el precio de spot más bajo.
- [VPC no predeterminada] Debe especificar la subred para la instancia de spot.

Historial de precios de instancias de spot

Amazon EC2 define los precios de las instancias de spot y estos se ajustan gradualmente en función de las tendencias a largo plazo de la oferta y la demanda de capacidad de este tipo de instancia.

Cuando su solicitud se haya completado, sus instancias de spot se inician al precio de spot, sin exceder el precio bajo demanda. Puede ver el historial del precio de spot para los últimos 90 días, filtrando por tipo de instancia, sistema operativo y zona de disponibilidad.

Para ver los precios de spot actuales

Para conocer los precios actuales de las instancias de spot, consulte Precios de instancias de spot de Amazon EC2.

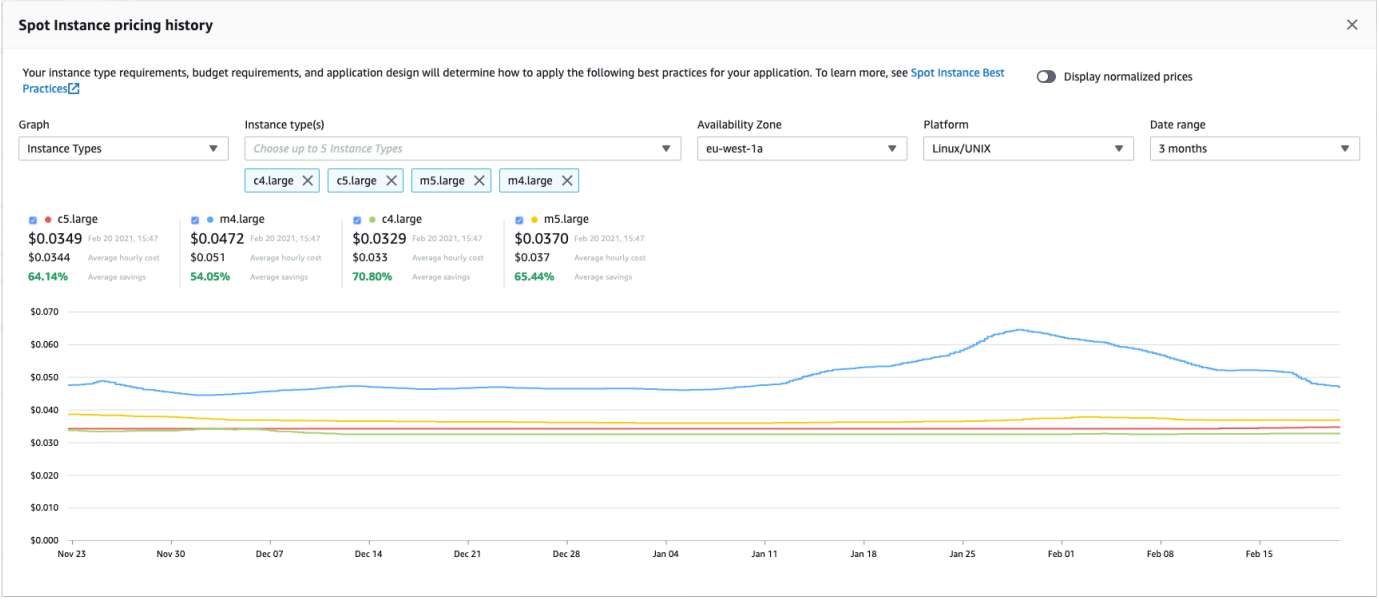
Para ver el historial de precios de spot a través de la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Spot Requests (Solicitudes de spot).
3. Elija Historial de precios.

4. En Graph (Gráfico), seleccione para comparar el historial de precios por Availability Zones (Zonas de disponibilidad) o por Instance Types (Tipos de instancia).

   - Si elige Availability Zones (Zonas de disponibilidad), entonces elija el Instance type (Tipo de instancia), el sistema operativo (Platform [Plataforma]) y el Date range (Intervalo de fechas) cuyo historial de precios desea ver.
   - Si elige Instance Types (Tipos de instancias), entonces elija hasta cinco Instance type(s) (Tipo[s] de instancia[s]), la Availability Zone (Zona de disponibilidad), el sistema operativo (Platform [Plataforma]) y el Date range (Intervalo de fechas) cuyo historial de precios desea ver.

   La siguiente captura de pantalla muestra una comparación de precios para diferentes tipos de instancias.



5. Coloque (o mueva) el puntero sobre el gráfico para mostrar los precios a horas específicas en el rango de fechas seleccionado. Los precios se muestran en los bloques de información sobre el gráfico. El precio mostrado en la fila superior muestra el precio en una fecha específica. El precio mostrado en la segunda fila muestra el precio medio en el intervalo de fechas seleccionado.
6. Para mostrar el precio por vCPU, active Display normalized prices (Mostrar precios normalizados). Para mostrar el precio del tipo de instancia, desactive Display normalized prices (Mostrar precios normalizados).

Para ver el historial de precios de spot mediante la línea de comandos

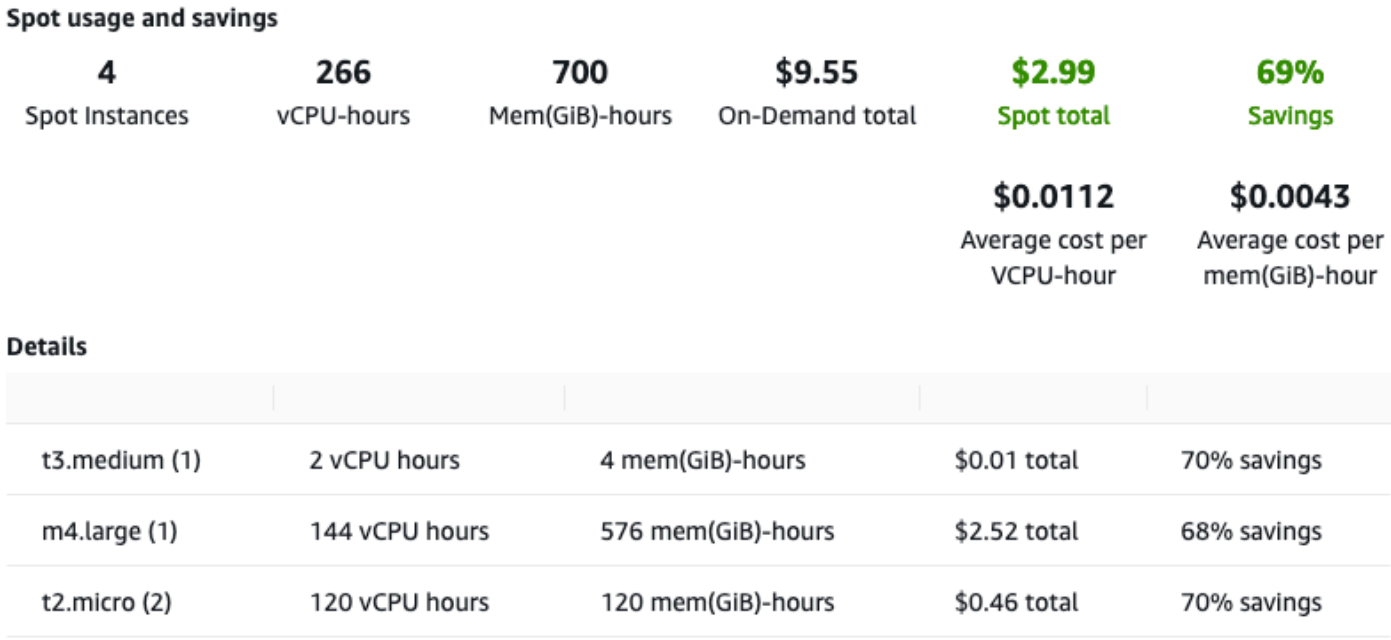
Puede utilizar uno de los siguientes comandos. Para obtener más información, consulte Acceder a Amazon EC2.

- describe-spot-price-history (AWS CLI)
- Get-EC2SpotPriceHistory (AWS Tools for Windows PowerShell)

Ahorro en la compra de instancias de spot

Puede ver la información sobre el uso y el ahorro de las instancias de spot en el nivel de cada flota o de todas las instancias de spot en ejecución. En el nivel de cada flota, la información sobre el uso y el ahorro incluye todas las instancias iniciadas y terminadas por la flota. Puede ver esta información de la última hora o de los últimos tres días.

En la siguiente captura de pantalla de la sección Savings (Ahorros), se muestra la información del uso y el ahorro de spot de una flota de spot.



Puede ver la siguiente información de uso y de ahorro:

- “Spot instances” (instancias de spot): La cantidad de instancias puntuales iniciadas y terminadas por la flota de spot. Al ver el resumen del ahorro, el número representa todas las instancias de spot en ejecución.

- vCPU-hours (Horas de CPU virtual) –: número de horas de la CPU virtual utilizadas en todas las instancias de spot en el período de tiempo seleccionado.
- Mem(GiB)-hours (Horas de memoria (GiB)):– número de horas de GiB utilizadas en todas las instancias de spot en el período de tiempo seleccionado.
- On-Demand total (Total bajo demanda):– cantidad total pagada por el período de tiempo seleccionado si estas instancias se hubieran iniciado como instancias bajo demanda.
- Spot total (Total de spot):– cantidad total a pagar por el período de tiempo seleccionado.
- Savings (Ahorro):– porcentaje de ahorro al no pagar un precio bajo demanda.
- Average cost per vCPU-hour (Costo medio por hora de CPU virtual):– costo medio por hora del uso de la CPU virtual en todas las instancias de spot durante el período de tiempo seleccionado y calculado del siguiente modo: Average cost per vCPU-hour (Costo medio por hora de CPU virtual) = Spot total (Total de spot) / vCPU-hours (Horas de CPU virtual).
- Average cost per mem(GiB)-hour (Costo medio por hora de memoria (GiB):– costo medio por hora del uso de GiB en todas las instancias de spot durante el período de tiempo seleccionado y calculado del siguiente modo: Average cost per mem(GiB)-hour (Costo medio por hora de CPU virtual) = Spot total (Total de spot) / Mem(GiB)-hours (Horas de memoria (GiB)).
- Tabla “Details” (Detalles): los distintos tipos de instancia (cantidad de instancias por tipo de instancia entre paréntesis) que incluye la flota de spot. En el resumen del ahorro se incluyen todas las instancias de spot en ejecución.

La información del ahorro solo puede verse con la consola de Amazon EC2.

Para ver la información de ahorro de una flota de spot a través de la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Spot Requests (Solicitudes de spot).
3. Seleccione el ID de una solicitud de flota de spot y desplácese hasta la sección Savings (Ahorros).

   Como alternativa, seleccione la casilla situada junto al ID de la solicitud de flota de spot y, a continuación, elija la pestaña Savings (Ahorros).
4. De forma predeterminada, la página muestra la información de uso y de ahorro de los últimos tres días. Puede elegir la última hora o los últimos tres días. Para las Flotas de spot iniciadas hace menos de una hora, la página muestra el ahorro previsto de dicha hora.

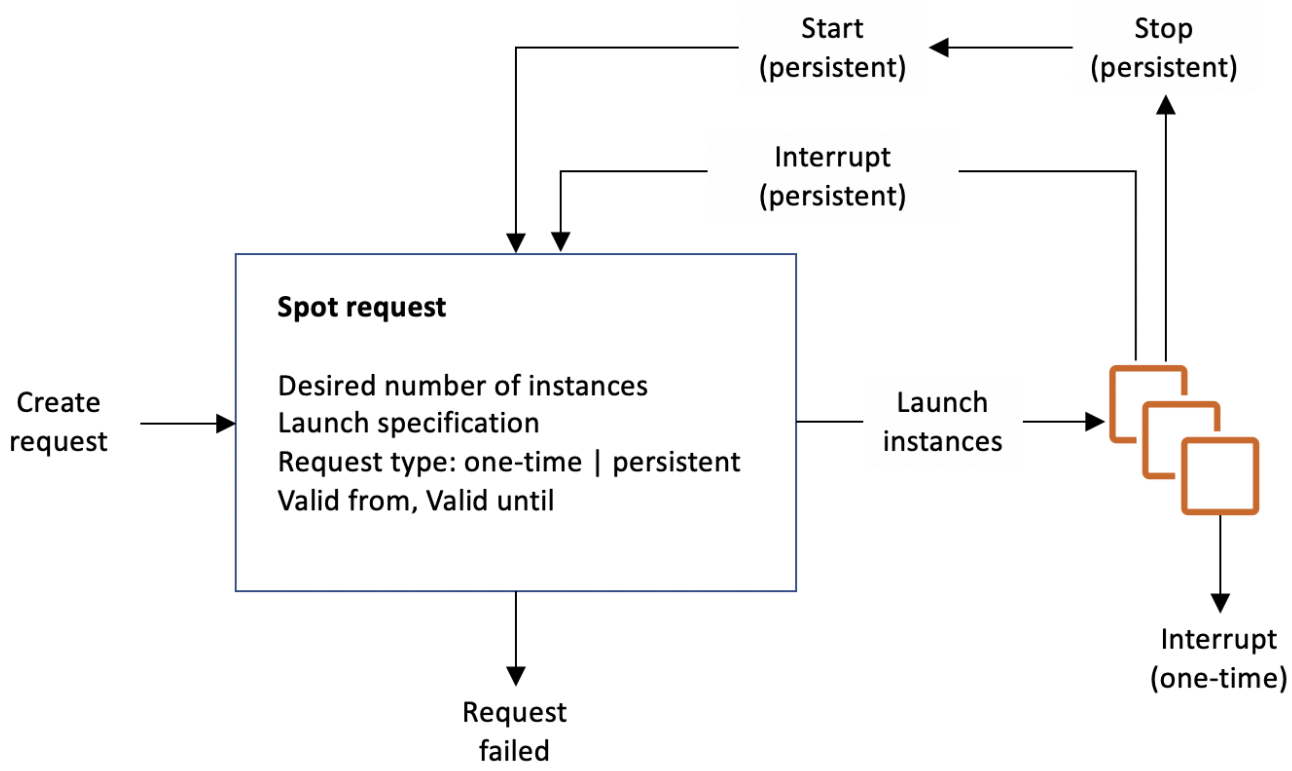
Para ver la información de ahorro de todas las instancias de spot en ejecución a través de la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Spot Requests (Solicitudes de spot).
3. Seleccione Savings Summary (Resumen de ahorro).

Trabajar con instancias de spot

Para utilizar las instancias de spot, crea una solicitud de instancia de spot que incluye la cantidad de instancias deseada, el tipo de instancia y la zona de disponibilidad. Si hay capacidad disponible, Amazon EC2 satisface su solicitud de manera inmediata. De lo contrario, Amazon EC2 espera hasta que pueda atender su solicitud o hasta que usted la cancele.

En la siguiente ilustración, se muestra cómo funcionan las solicitudes de instancias de spot. Observe que el tipo de solicitud (por única vez o persistente) determina si la solicitud se abre de nuevo cuando Amazon EC2 interrumpe una instancia de spot o si usted detiene una instancia de spot. Si la solicitud es persistente, después de interrumpir la instancia de spot, se volverá a abrir la solicitud. Si la solicitud es persistente y detiene su instancia de spot, la solicitud solo se abre después de iniciar su instancia de spot.



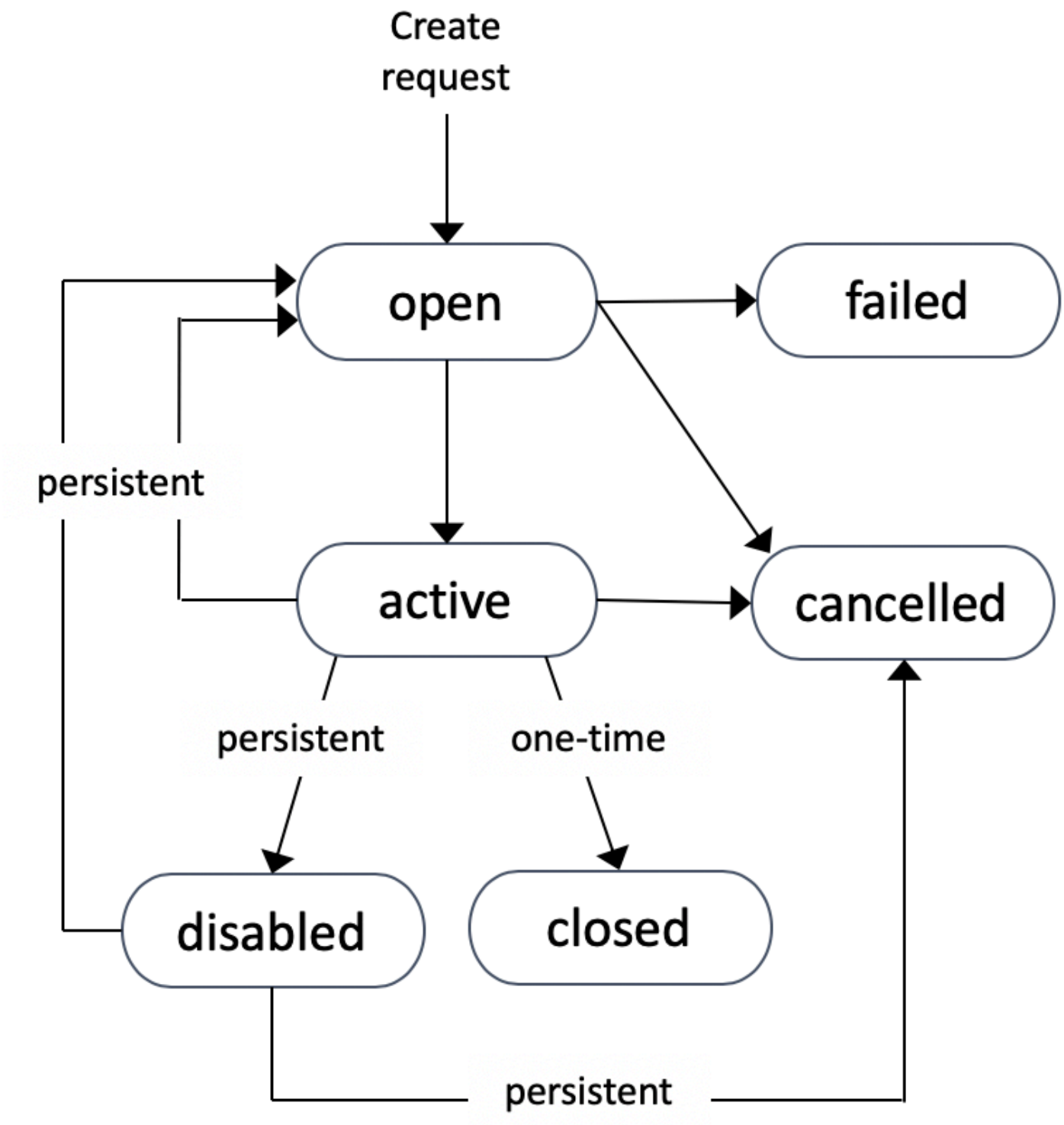
Contenido

Estados de las solicitudes de instancia de spot

Una solicitud de instancia de spot puede tener uno de los siguientes estados:

- `open`: la solicitud aún debe completarse.
- `active`: la solicitud se ha completado y tiene una instancia de spot asociada.
- `failed`: la solicitud tiene uno o varios parámetros incorrectos.
- `closed`: la instancia de spot se ha interrumpido o terminado.
- `disabled`: ha detenido la instancia de spot.
- `cancelled`: ha cancelado la solicitud o la solicitud ha caducado.

La siguiente ilustración representa las transiciones entre los distintos estados de una solicitud. Tenga en cuenta que las transiciones dependen de si el tipo de solicitud es de una única vez o persistente.



Una solicitud de instancia por única vez permanece activa hasta que Amazon EC2 inicia la instancia de spot, la solicitud caduca o el usuario la cancela. Si no hay capacidad disponible, la instancia de spot se termina y la solicitud de instancia de spot se cierra.

Una solicitud de instancia de spot persistente permanece activa hasta que caduca o hasta que el usuario la cancela, incluso si se cumple la solicitud. Si no hay capacidad disponible, la instancia de spot se interrumpe. Una vez interrumpida la instancia, cuando vuelve a disponer de capacidad, la instancia de spot se inicia si se había detenido o se reanuda si estaba hibernando. Puede detener una instancia de spot e iniciarla de nuevo si la capacidad está disponible. Si se termina la instancia de spot (con independencia de si la instancia de spot está en un estado detenido o en ejecución), la solicitud de instancia de spot se abre de nuevo y Amazon EC2 inicia una nueva instancia de spot. Para obtener más información, consulte Detener una instancia de spot, Iniciar una instancia de spot y Terminar una instancia de spot.

Puede realizar el seguimiento del estado de las solicitudes de instancia de spot, así como del estado de las instancias de spot iniciadas, a través del estado. Para obtener más información, consulte Estado de las solicitudes de spot.

Especificar una tenencia para su instancias de spot

Puede ejecutar una instancia de spot en hardware de inquilino único. Las instancias de spot dedicadas están aisladas físicamente de las instancias que pertenecen a otras cuentas de AWS. Para obtener más información, consulte Dedicated Instances y la página del producto instancias dedicadas de Amazon EC2.

Para ejecutar una instancia de spot dedicada, realice una de las siguientes operaciones:

- Cuando cree la solicitud de instancia de spot, especifique una tenencia `dedicated`. Para obtener más información, consulte Crear una solicitud de instancia de spot.
- Solicite una instancia dedicada en una VPC con una tenencia de instancia `dedicated`. Para obtener más información, consulte Creación de una VPC con una tenencia de una instancia dedicada. No puede solicitar una instancia dedicada con una tenencia `default` si la solicitó en una VPC con una tenencia de instancia `dedicated`.

Todas las familias de instancias admiten instancias de spot dedicadas excepto instancias T. Para cada familia de instancias admitidas, solo la instancia o metal de mayor tamaño admite instancias de spot dedicadas.

Rol vinculado al servicio para solicitudes de instancias de spot

Amazon EC2 utiliza roles vinculados a un servicio para los permisos que necesita para llamar a otros servicios de AWS en su nombre. Un rol vinculado a un servicio es un tipo único de rol de IAM que

está vinculado directamente a un servicio de AWS. Los roles vinculados a servicios ofrecen una manera segura de delegar permisos a los servicios de AWS, ya que solo los servicios vinculados pueden asumir roles vinculados a servicios. Para obtener más información, consulte Uso de roles vinculados a servicios en la Guía del usuario de IAM.

Amazon EC2 usa el rol vinculado a un servicio denominado AWSServiceRoleForEC2Spot para lanzar y administrar Instancias de spot en su nombre.

Permisos concedidos por AWSServiceRoleForEC2Spot

Amazon EC2 usa AWSServiceRoleForEC2Spot para ejecutar las acciones siguientes:

- `ec2:DescribeInstances`: describir instancias de spot
- `ec2:StopInstances`: detener instancias de spot
- `ec2:StartInstances`: iniciar instancias de spot

Creación del rol vinculado a servicio

En la mayoría de los casos, no es necesario crear manualmente roles vinculados a servicios. Amazon EC2 crea el rol vinculado a un servicio AWSServiceRoleForEC2Spot la primera vez que se solicita una instancia de spot mediante la consola.

Si tenía una solicitud de instancia de spot activa antes de octubre de 2017, cuando Amazon EC2 empezó a admitir este rol vinculado a servicio, Amazon EC2 creó el rol AWSServiceRoleForEC2Spot en su cuenta de AWS. Para obtener más información, consulte Un nuevo rol ha aparecido en mi cuenta en la Guía del usuario de IAM

Si utiliza la AWS CLI o una API para realizar una solicitud de instancias de spot, debe asegurarse de que este rol exista.

Cómo crear AWSServiceRoleForEC2Spot mediante la consola

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. Seleccione Roles en el panel de navegación.
3. Elija Create role.
4. En la página Seleccionar el tipo de entidad de confianza, elija EC2, EC2: instancias de spot y Siguiente: Permisos.
5. En la siguiente página, elija Next:Review (Siguiente: Revisión).

6. En la página Review (Revisión), elija Create role (Crear rol).

Cómo crear AWSServiceRoleForEC2Spot con la AWS CLI

Utilice el comando create-service-linked-role de la siguiente manera.

```
aws iam create-service-linked-role --aws-service-name spot.amazonaws.com
```

Si ya no tiene que utilizar instancias de spot, le recomendamos que elimine el rol AWSServiceRoleForEC2Spot. Después de eliminar este rol de la cuenta, Amazon EC2 volverá a crearlo cuando solicite instancias de spot.

Conceder acceso a las claves administradas por el cliente para su uso con AMI cifradas e instantáneas de EBS

Si especifica una AMI cifrada o una instantánea de Amazon EBS cifrada en sus instancias de spot y usa una clave administrada por el cliente para el cifrado, debe conceder permiso al rol AWSServiceRoleForEC2Spot para que use esa clave a fin de que Amazon EC2 pueda iniciar instancias de spot en su nombre. Para ello, debe agregar una concesión a la clave administrada por el cliente, como se muestra en el siguiente procedimiento.

Al proporcionar permisos, las concesiones son una alternativa a las políticas de claves. Para obtener más información, consulte Uso de concesiones y Uso de políticas de claves en AWS KMS en la Guía para desarrolladores de AWS Key Management Service.

Para conceder permisos al rol AWSServiceRoleForEC2Spot a fin de que utilice la clave administrada por el cliente

- Use el comando create-grant para agregar una concesión a la clave administrada por el cliente y para especificar la entidad principal (el rol vinculado a un servicio AWSServiceRoleForEC2Fleet) que recibe permiso para realizar las operaciones que permite la concesión. La clave administrada por el cliente se especifica mediante el parámetro `key-id` y el ARN de la clave administrada por el cliente. La entidad principal se especifica con el parámetro `grantee-principal` y el ARN del rol vinculado a un servicio AWSServiceRoleForEC2Spot.

  ```
  aws kms create-grant \
      --region us-east-1 \
      --key-id arn:aws:kms:us-
  east-1:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab \
  ```

```
    --grantee-principal arn:aws:iam::111122223333:role/aws-service-role/
spot.amazonaws.com/AWSServiceRoleForEC2Spot \
    --operations "Decrypt" "Encrypt" "GenerateDataKey"
 "GenerateDataKeyWithoutPlaintext" "CreateGrant" "DescribeKey" "ReEncryptFrom"
 "ReEncryptTo"
```

Crear una solicitud de instancia de spot

Puede utilizar el asistente de inicialización de instancias en la consola de Amazon EC2 o el comando de la AWS CLI run-instances para solicitar una instancia de spot del mismo modo que puede iniciar una instancia bajo demanda. Este método solo se recomienda por las razones siguientes:

- Ya está utilizando el asistente de inicialización de instancias o el comando run-instances para iniciar instancias bajo demanda, y simplemente desea hacer un cambio para iniciar instancias de spot mediante la modificación de un solo parámetro.
- No necesita varias instancias con distintos tipos de instancias.

Por lo general, este método no se recomienda para iniciar instancias de spot porque no se puede especificar varios tipos de instancias y no puede iniciar instancias de spot e instancias bajo demanda en la misma solicitud. Para conocer los métodos preferidos para iniciar instancias de spot, que incluyen la inicialización de una flota que, a su vez, incluye instancias de spot e instancias bajo demanda con varios tipos de instancias, consulte ¿Cuál es el mejor método de solicitud de spot que se puede utilizar?

Si solicita varias instancias de spot a la vez, Amazon EC2 crea solicitudes de instancia de spot independientes, lo que permite realizar el seguimiento del estado de cada una por separado. Para obtener más información acerca de las instancias de spot, consulte Estado de las solicitudes de spot.

New console

Para crear una solicitud de instancia de spot mediante el asistente de inicialización de instancias

Los pasos del 1 al 9 son los mismos pasos que usaría para iniciar una instancia bajo demanda. En el paso 10, configura la solicitud de instancia de spot.

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la barra de navegación de la parte superior de la pantalla, seleccione una región.
3. En el panel de la consola de Amazon EC2, elija iniciar instancia .

4. (Opcional) En Name and tags (Nombre y etiquetas), puede nombrar la instancia y etiquetar la solicitud de instancia de spot, la instancia, los volúmenes y los gráficos elásticos. Para obtener más información acerca de las etiquetas, consulte Etiquetar los recursos de Amazon EC2.

   a. En Name (Nombre), ingrese un nombre descriptivo para la instancia.

      El nombre de la instancia es una etiqueta, donde la clave es Name (Nombre) y el valor es el nombre que especifique. Si no especifica un nombre, la instancia se puede identificar mediante su ID, que se genera automáticamente al iniciar la instancia.

   b. Elija Add additional tags (Agregar etiquetas adicionales) para etiquetar la solicitud de instancia de spot, la instancia, los volúmenes y los gráficos elásticos. Elija Add tag (Agregar etiqueta) y, a continuación, ingrese una clave y un valor, y seleccione el tipo de recurso que desea etiquetar. Elija Add tag (Agregar etiqueta) para cada etiqueta adicional.

5. En Application and OS Images (Amazon Machine Image) (Imágenes de aplicaciones y sistema operativo [Imagen de máquina de Amazon]), elija el sistema operativo (SO) para la instancia y luego, seleccione una AMI. Para obtener más información, consulte Imágenes de aplicaciones y sistema operativo (Imagen de máquina de Amazon).

6. En Instance type (Tipo de instancia), seleccione el tipo de instancia que cumpla con los requisitos para la configuración de hardware y el tamaño de la instancia. Para obtener más información, consulte Tipo de instancia.

7. En Key pair (login) (Par de claves [inicio de sesión]), elija un par de claves existente o elija Create new key pair (Crear par de claves nuevo) para crear uno nuevo. Para obtener más información, consulte Pares de claves e instancias de Amazon EC2.

   > **Important**
   >
   > Si elige la opción Proceed without key pair (Not recommended) (Continuar sin un par de claves [No recomendado]), no podrá conectarse a la instancia a menos que elija una AMI que esté configurada para ofrecer a los usuarios otra forma de iniciar sesión.

8. En Network settings (Configuración de red), utilice la configuración predeterminada o elija Edit (Editar) para configurar los ajustes de red según sea necesario.

Los grupos de seguridad forman parte de la configuración de la red y definen las reglas del firewall para la instancia. Estas reglas especifican qué tráfico procedente de la red se entregará en la instancia.

Para obtener más información, consulte Network settings (Configuración de red).

9. La AMI que seleccione incluye uno o más volúmenes de almacenamiento, incluido el volumen de dispositivo raíz. En Configure storage (Configurar almacenamiento), puede especificar los volúmenes adicionales que desea adjuntar a la instancia mediante Add new volume (Agregar volumen nuevo). Para obtener más información, consulte Configurar almacenamiento.
10. En Advanced details (Detalles avanzados), configure la solicitud de instancia de spot de la siguiente manera:

    a. En Purchasing option (Opción de compra), seleccione la casilla de verificación Request Spot Instances (Solicitar instancias de spot).

    b. Puede conservar la configuración predeterminada para la solicitud de instancia de spot o elegir Customize (Personalizar) (a la derecha) para especificar la configuración personalizada para la solicitud de instancia de spot.

    Cuando elige Customize (Personalizar), aparecen los siguientes campos.

    i. Maximum price (Precio máximo): puede solicitar instancias de spot al precio de spot, limitado al precio bajo demanda, o puede especificar el monto máximo que está dispuesto a pagar.

    > **Warning**
    >
    > Si especifica un precio máximo, las instancias se interrumpirán con más frecuencia que si elige Sin precio máximo.

    - No maximum price (Sin precio máximo): la instancia de spot se iniciará al precio de spot actual. El precio nunca superará el precio bajo demanda. (Recomendado)
    - Set your maximum price (Establecer el precio máximo [por instancia/por hora]): puede especificar el monto máximo que está dispuesto a pagar.

- Si especifica un precio máximo inferior al precio de spot actual, la instancia de spot no se iniciará.
- Si especifica un precio máximo superior al precio de spot actual, su instancia de spot se iniciará y se cobrará al precio de spot actual. Una vez que la instancia de spot está en ejecución, si el precio de spot supera el precio máximo, Amazon EC2 interrumpe la instancia de spot.
- Independientemente del precio máximo que especifique, siempre se le cobrará el precio de spot actual.

Para revisar las tendencias de los precios de spot, consulte Historial de precios de instancias de spot.

ii. Request type (Tipo de solicitud): el tipo de solicitud de instancia de spot que elija determina qué ocurre si la instancia de spot se interrumpe.

- Por única vez: Amazon EC2 realiza una solicitud por única vez para su instancia de spot. Si la instancia de spot se interrumpe, la solicitud no se vuelve a enviar.
- Solicitud persistente: Amazon EC2 realiza una solicitud persistente para su instancia de spot. Si la instancia de spot se interrumpe, se vuelve a enviar la solicitud para reponer la instancia de spot que se interrumpió.

Si no se especifica un valor, el predeterminado es una solicitud por única vez.

iii. Válido para (Válido hasta): la fecha de vencimiento de una solicitud persistente de instancia de spot.

Este campo no se admite para solicitudes por única vez. Una solicitud por única vez permanece activa hasta que se inician todas las intancias de la solicitud o hasta que se cancela la solicitud.

- No request expiry date (Sin fecha de vencimiento de solicitud): la solicitud permanece activa hasta que se cancela.
- Set your request expiry date (Fijar la fecha de vencimiento de la solicitud): la solicitud persistente permanece activa hasta la fecha especificada o hasta que se cancela.

iv. Interruption behavior (Comportamiento de interrupción): el comportamiento que elija determinará qué ocurrirá cuando una instancia de spot se interrumpa.

- En el caso de solicitudes persistentes, los valores válidos son Stop (Detener) e Hibernate (Hibernar). Cuando se detiene una instancia, se aplican cargos por almacenamiento de volumen de EBS.

  > **Note**
  >
  > Las instancias de spot utilizan ahora la misma funcionalidad de hibernación que las instancias bajo demanda. Para habilitar la hibernación, puede seleccionar Hibernar aquí o Habilitar en el campo de Detener: comportamiento de hibernación, que aparece más abajo en el asistente de inicialización de instancias. Para conocer los requisitos previos de hibernación, consulte Requisitos previos para la hibernación de instancias de Amazon EC2.

- En el caso de solicitudes por única vez, solo Terminate (Terminar) es válido.

Si no se especifica un valor, el predeterminado es Terminar, el cual no es válido para las solicitudes de instancia de spot persistentes. Si se mantiene el valor predeterminado y se intenta iniciar una solicitud de instancia de spot persistente, se producirá un error.

Para obtener más información, consulte Comportamiento de las interrupciones de las instancias de spot.

11. En el panel Resumen, en Cantidad de instancias, escriba la cantidad de instancias que iniciará.

    > **Note**
    >
    > Amazon EC2 crea una solicitud independiente para cada instancia de spot.

12. En el panel Summary (Resumen), revise los detalles de la instancia y realice los cambios necesarios. Después de enviar la solicitud de instancia de spot, no podrá cambiar los parámetros de la solicitud. Puede navegar directamente a una sección del asistente de inicialización de instancias mediante la selección del enlace correspondiente en el panel Summary (Resumen). Para obtener más información, consulte Resumen.
13. Cuando lo tenga todo listo para iniciar una instancia, elija iniciar instancia.

Si se produce un error al iniciar la instancia o el estado pasa inmediatamente a `terminated` en lugar de `running`, consulte Solucionar problemas de lanzamiento de instancias.

Old console

Para crear una solicitud de instancia de spot mediante el asistente de inicialización de instancias

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la barra de navegación de la parte superior de la pantalla, seleccione una región.
3. En el panel de la consola de Amazon EC2, elija Iniciar instancia.
4. En la página Elegir una Imagen de máquina de Amazon (AMI), elija una AMI. Para obtener más información, consulte Paso 1: Elegir una Imagen de máquina de Amazon (AMI).
5. En la página Choose an Instance Type (Elegir un tipo de instancia), seleccione la configuración de hardware y el tamaño de la instancia que desea iniciar y luego, elija Next: Configure Instance Details (Siguiente: configurar detalles de instancia). Para obtener más información, consulte Paso 2: Elegir un tipo de instancia.
6. En la página Configurar detalles de instancia configure la solicitud de instancias de spot de la siguiente manera:

   - Number of instances (Número de instancias): escriba el número de instancias que desea iniciar.

     > **Note**
     >
     > Amazon EC2 crea una solicitud independiente para cada instancia de spot.

   - (Opcional) Para ayudar a garantizar que se mantenga el número correcto de instancias para satisfacer la demanda de la aplicación, puede elegir Launch into Auto Scaling Group (iniciar en grupo de Auto Scaling) para crear una configuración de inicialización y un grupo de Auto Scaling. Auto Scaling escala el número de instancias en el grupo según sus especificaciones. Para obtener más información, consulte la Guía del usuario de Amazon EC2 Auto Scaling.
   - Purchasing option (Opción de compra): elija Request Spot instances (Solicitar instancias de spot) para iniciar una instancia spot. Al elegir esta opción, aparecen los siguientes campos.

- Precio actual: se muestra el precio de spot actual en cada zona de disponibilidad para el tipo de instancia seleccionado.
- (Opcional) Precio máximo: puede dejar el campo vacío o puede especificar el importe máximo que está dispuesto a pagar.

> **Warning**
>
> Si especifica un precio máximo, las instancias se interrumpirán con más frecuencia que si deja el campo vacío.

  - Si especifica un precio máximo que es inferior al precio de spot, su instancia de spot no se iniciará.
  - Si especifica un precio máximo que es superior al precio de spot actual, su instancia de spot se iniciará y se cobrará al precio de spot actual. Una vez que la instancia de spot está en ejecución, si el precio de spot supera el precio máximo, Amazon EC2 interrumpe la instancia de spot.
  - Independientemente del precio máximo que especifique, siempre se le cobrará el precio de spot actual.
  - Si deja el campo vacío, pagará el precio de spot actual.
- Solicitud persistente: elija Persistent request (Solicitud persistente) para volver a enviar la solicitud de instancia de spot si esta se ve interrumpida.
- Comportamiento de interrupción: de forma predeterminada, el servicio de Spot termina una instancia de spot cuando se interrumpe. Si elige Persistent request (Solicitud persistente), puede especificar que el servicio de Spot detenga o hiberne la instancia de spot cuando se interrumpa. Para obtener más información, consulte Comportamiento de las interrupciones de las instancias de spot.
- (Opcional) Solicitud válida para: elija Edit (Editar) para especificar cuándo caduca la solicitud de instancia de spot.

Para obtener más información sobre cómo configurar una instancia de spot, consulte Paso 3: Configurar los detalles de la instancia

7. La AMI que seleccione incluye uno o más volúmenes de almacenamiento, incluido el volumen de dispositivo raíz. En la página Add Storage (Añadir almacenamiento), puede especificar los volúmenes adicionales que desea adjuntar a la instancia eligiendo Add New

Volume (Añadir nuevo volumen). Para obtener más información, consulte Paso 4: Agregar almacenamiento.

8. En la página Add Tags (Añadir etiquetas), especifique etiquetas proporcionando combinaciones de clave y valor. Para obtener más información, consulte Paso 5: Añadir etiquetas.
9. En la página Configure Security Group (Configurar grupo de seguridad), utilice un grupo de seguridad para definir reglas de firewall para la instancia. Estas reglas especifican qué tráfico procedente de la red se entregará en la instancia. El resto del tráfico se ignora. (Para obtener más información acerca de los grupos de seguridad, consulte Grupos de seguridad de Amazon EC2 para instancias EC2.) Seleccione o cree un grupo de seguridad y, a continuación, elija Revisar y iniciar. Para obtener más información, consulte Paso 6: Configurar un grupo de seguridad.
10. En la página Review Instance Launch (Revisar inicialización de instancia), compruebe los detalles de la instancia y haga los cambios necesarios seleccionando el enlace Edit (Editar) correspondiente. Cuando esté preparado, elija Launch (iniciar). Para obtener más información, consulte Paso 7: Revisar la inicialización de la instancia y seleccionar el par de claves.
11. En el cuadro de diálogo Select an existing key pair or create a new key pair (Seleccionar par de claves existentes o crear nuevo par de claves), puede elegir un par de claves existente o crear uno nuevo. Por ejemplo, elija Elegir un par de claves existente y, a continuación, seleccione el par de claves que creó al obtener la configuración. Para obtener más información, consulte Pares de claves e instancias de Amazon EC2.

    > **Important**
    >
    > Si elige la opción Proceed without key pair (Continuar sin un par de claves), no podrá conectarse a la instancia a menos que elija una AMI que esté configurada para ofrecer a los usuarios otra forma de iniciar sesión.

12. Para iniciar la instancia, active la casilla de verificación de confirmación y, a continuación, elija Launch Instances (iniciar instancias).

    Si se produce un error al lanzar la instancia o el estado pasa inmediatamente a `terminated` en lugar de `running`, consulte Solucionar problemas de lanzamiento de instancias.

AWS CLI

Para crear una solicitud de instancia de spot mediante run-instances

Utilice el comando run-instances (Ejecutar instancias) y especifique las opciones de instancia de spot en el parámetro `--instance-market-options`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type t2.micro \
    --count 5 \
    --subnet-id subnet-08fc749671b2d077c \
    --key-name MyKeyPair \
    --security-group-ids sg-0b0384b66d7d692f9 \
    --instance-market-options file://spot-options.json
```

La siguiente es la estructura de datos para especificar en el archivo JSON para `--instance-market-options`. También puede especificar `ValidUntil` y `InstanceInterruptionBehavior`. Si no especifica un campo en la estructura de datos, se utiliza el valor predeterminado.

El siguiente ejemplo crea una solicitud `persistent`.

```
{
  "MarketType": "spot",
  "SpotOptions": {
    "SpotInstanceType": "persistent"
  }
}
```

Para crear una solicitud de instancia de spot mediante request-spot-instances

> **Note**
>
> Se desaconseja utilizar el comando request-spot-instances para solicitar una instancia de spot, ya que es una API heredada sin inversión planificada. Para obtener más información, consulte ¿Cuál es el mejor método de solicitud de spot que se puede utilizar?.

Utilice el comando request-spot-instances para crear una solicitud puntual:

```
aws ec2 request-spot-instances \
    --instance-count 5 \
    --type "one-time" \
    --launch-specification file://specification.json
```

Utilice el comando request-spot-instances para crear una solicitud persistente.

```
aws ec2 request-spot-instances \
    --instance-count 5 \
    --type "persistent" \
    --launch-specification file://specification.json
```

Para ver archivos de especificación de inicialización que utilizan estos comandos, consulte Ejemplo de especificaciones de inicialización de solicitudes de instancia de spot. Si descarga un archivo de especificación de inicialización desde la consola de la solicitud de spot, debe utilizar el comando request-spot-fleet en su lugar (la consola de la solicitud de spot especifica una solicitud de instancia de spot mediante una flota de spot).

Búsqueda de instancias de spot

Amazon EC2 ejecuta una instancia de spot siempre que haya capacidad disponible. Una instancia de spot se ejecuta hasta que se interrumpe o usted la termina.

En la página Instancias de la consola, una instancia de spot aparece junto con las instancias bajo demanda. Utilice el procedimiento que se muestra a continuación para encontrar instancias de spot.

Console

Para encontrar las instancias de spot a través de la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Para encontrar todas las instancias de spot, en el panel de búsqueda seleccione Ciclo de vida de instancia=spot.
4. Para verificar que una instancia sea una de spot, seleccione la instancia, luego vaya a la pestaña Detalles y compruebe el valor de Ciclo de vida. El valor de una instancia de spot es `spot` y el valor de una instancia bajo demanda es `normal`.

AWS CLI

Para encontrar instancias de spot a través de la AWS CLI

Utilice el comando describe-instances con la opción `--filters`.

```
aws ec2 describe-instances \
    --filters "Name=instance-lifecycle,Values=spot"
```

Para determinar si una instancia es una instancia de spot

Utilice el comando describe-instances con la opción `--query` para comprobar el valor del ciclo de vida.

```
aws ec2 describe-instances \
    --instance-ids i-0123a456700123456 \
    --query "Reservations[*].Instances[*].InstanceLifecycle" \
    --output text
```

Si la salida es `spot`, la instancia es una instancia de spot. Si no hay salida, la instancia es una instancia bajo demanda.

Utilice el procedimiento que se muestra a continuación para encontrar instancias de spot lanzadas desde una solicitud de una instancia de spot o una flota de spot específica.

Console

Para encontrar las instancias de spot de una solicitud a través de la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Solicitudes de spot. La lista incluye tanto las solicitudes de las instancias de spot como las de las flotas de spot.
3. Si se cumple con una solicitud de una instancia de spot, el ID de la instancia de spot será Capacidad. Para una flota de spot, Capacity (Capacidad) indica qué cantidad de la capacidad solicitada se ha alcanzado. Para ver los ID de las instancias en una flota de spot, elija la flecha hacia arriba o seleccione la flota y, a continuación, seleccione Instances (instancia[s]).
4. En una flota de spot, Capacidad indica la cantidad de la capacidad solicitada que se ha alcanzado. Para ver los ID de las instancias de una flota de spot, seleccione el ID de la flota. Cuando se abra la página de detalles, busque el panel Instancias.

AWS CLI

Para encontrar las instancias de spot de una solicitud a través de la AWS CLI

Utilice el comando describe-spot-instance-requests con la opción `--query`.

```
aws ec2 describe-spot-instance-requests \
    --query "SpotInstanceRequests[*].{ID:InstanceId}"
```

A continuación, se muestra un ejemplo de la salida:

```
[
    {
        "ID": "i-1234567890abcdef0"
    },
    {
        "ID": "i-0598c7d356eba48d7"
    }
]
```

Etiquetar las solicitudes de instancia de spot

Para ayudarlo a clasificar y a administrar las solicitudes de instancia de spot, puede etiquetarlas con metadatos personalizados. Puede asignar una etiqueta a una solicitud de instancia de spot cuando la cree o posteriormente. Puede asignar etiquetas mediante la consola de Amazon EC2 o una herramienta de línea de comandos.

Al etiquetar una solicitud de instancia de spot, las instancias y los volúmenes iniciados por la solicitud de instancia de spot no se etiquetan automáticamente. Tiene que etiquetar de manera explícita las instancias y los volúmenes iniciados por la solicitud de instancia de spot. Puede asignar una etiqueta a una instancia de spot y a los volúmenes durante la inicialización o después.

Para obtener más información sobre cómo funcionan las etiquetas, consulte Etiquetar los recursos de Amazon EC2.

Contenido

- Etiquetar una solicitud de instancia de spot existente
- Ver las etiquetas de las solicitudes de instancias de spot

Requisitos previos

Otorgue al usuario el permiso para etiquetar recursos. Para obtener más información acerca de las políticas de IAM y las políticas de ejemplo, consulte Ejemplo: Etiquetar recursos.

La política de IAM que cree se determina con el método que utilice para crear una solicitud de instancia de spot.

- Si utiliza el launch wizard de instancias o `run-instances` para solicitar instancias de spot, consulte To grant a user the permission to tag resources when using the launch instance wizard or run-instances.
- Si utiliza el comando `request-spot-instances` para solicitar instancias de spot, consulteTo grant a user the permission to tag resources when using request-spot-instances.

Para otorgar permiso a un usuario para etiquetar recursos cuando utilice el asistente de inicialización de instancias o instancias de ejecución

Cree una política de IAM que incluya lo siguiente:

- La acción `ec2:RunInstances`. Esto otorga al usuario permiso para iniciar una instancia.
- En `Resource`, especifique `spot-instances-request`. Esto permite a los usuarios crear solicitudes de instancias de spot, que solicitan instancias de spot.
- La acción `ec2:CreateTags`. Esto concede al usuario permiso para crear etiquetas.
- En `Resource`, especifique `*`. Esto permite a los usuarios etiquetar todos los recursos que se crean durante la inicialización de la instancia.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowLaunchInstances",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
```

```
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "TagSpotInstanceRequests",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Al utilizar la acción RunInstances para crear solicitudes de instancias de spot y etiquetar estas instancias durante la creación, debe tener en cuenta la manera en que Amazon EC2 evalúa el recurso `spot-instances-request` en la instrucción RunInstances. En la política de IAM, se evalúa de la siguiente manera:

- Si no etiqueta la solicitud de instancia de spot durante la creación, Amazon EC2 no evalúa el recurso `spot-instances-request` en la instrucción RunInstances.
- Si etiqueta la solicitud de instancia de spot durante la creación, Amazon EC2 evalúa el recurso `spot-instances-request` en la instrucción RunInstances.

Por lo tanto, para el recurso `spot-instances-request`, se aplican las siguientes reglas a la política de IAM:

- Si utiliza RunInstances para crear una solicitud de instancia de spot y no tiene la intención de etiquetar dicha solicitud durante la creación, no es necesario que permita explícitamente el recurso `spot-instances-request`; la llamada se realizará correctamente.
- Si utiliza RunInstances para crear una solicitud de instancia de spot y tiene la intención de etiquetar dicha solicitud durante la creación, debe incluir el recurso `spot-instances-request` en la instrucción de permiso de RunInstances; de lo contrario, la llamada devolverá un error.

- Si utiliza RunInstances para crear una solicitud de instancia de spot y tiene la intención de etiquetar dicha solicitud durante la creación, debe especificar el recurso `spot-instances-request` o incluir el comodín `*` en la instrucción de permiso de “CreateTags” (Crear etiquetas); de lo contrario, la llamada devolverá un error.

Para ejemplos de políticas de IAM, incluidas las políticas que no se admiten para las solicitudes de instancia de spot, consulte Trabajar con Instancias de spot.

Para conceder a un usuario el permiso para etiquetar recursos cuando utilice instancias de spot de solicitud

Cree una política de IAM que incluya lo siguiente:

- La acción `ec2:RequestSpotInstances`. Esto concede al usuario permiso para crear una solicitud de instancia de spot.
- La acción `ec2:CreateTags`. Esto concede al usuario permiso para crear etiquetas.
- En `Resource`, especifique `spot-instances-request`. Esto permite a los usuarios etiquetar solo la solicitud de instancia de spot.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "TagSpotInstanceRequest",
            "Effect": "Allow",
            "Action": [
                "ec2:RequestSpotInstances",
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:us-east-1:111122223333:spot-instances-request/*"
}
```

Etiquetar una nueva solicitud de instancia de spot

Console

Para etiquetar una nueva solicitud de instancia de spot mediante la consola

1. Siga el procedimiento indicado en Crear una solicitud de instancia de spot.

2. Para agregar una etiqueta, en la página Agregar etiquetas elija Agregar etiqueta y escriba la clave y el valor de la etiqueta. Elija Agregar otra etiqueta para cada etiqueta adicional.

   Para cada etiqueta, puede etiquetar la solicitud de instancia de spot, las instancias de spot y los volúmenes con la misma etiqueta. Para etiquetar los tres, asegúrese de que estén seleccionadas las Instances (instancia[s]), los Volumes (Volúmenes) y las Spot Instance Requests (Solicitudes de instancias de spot). Para etiquetar solo uno o dos, asegúrese de que los recursos que desea etiquetar están seleccionados y de que los demás recursos están borrados.

3. Rellene los campos necesarios para crear una solicitud de instancia de spot y, a continuación, elija Launch (iniciar). Para obtener más información, consulte Crear una solicitud de instancia de spot.

AWS CLI

Etiquetar una nueva solicitud de instancia de spot mediante la AWS CLI

Para etiquetar una solicitud de instancia de spot en la creación, configure los ajustes de la solicitud de instancia de spot de la siguiente manera:

- Especifique las etiquetas para la solicitud de instancias de spot mediante el parámetro `--tag-specification`.
- En `ResourceType`, especifique `spot-instances-request`. Si especifica otro valor, la solicitud de instancia de spot devolverá un error.
- Para `Tags`, especifique el par clave-valor. Puede especificar más de un par clave-valor.

En el siguiente ejemplo, la solicitud de instancia de spot se etiqueta con dos etiquetas: Key=Environment y Value=Production, además de Key=Cost-Center y Value=123.

```
aws ec2 request-spot-instances \
    --instance-count 5 \
    --type "one-time" \
    --launch-specification file://specification.json \
    --tag-specification 'ResourceType=spot-instances-
request,Tags=[{Key=Environment,Value=Production},{Key=Cost-Center,Value=123}]'
```

Etiquetar una solicitud de instancia de spot existente

Console

Para etiquetar una solicitud de instancia de spot existente mediante la consola

Después de crear una solicitud de instancia de spot, puede agregar etiquetas a la solicitud de instancia de spot a través de la consola.

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Solicitudes de spot.
3. Seleccione su solicitud de instancia de spot.
4. Elija la pestaña Tags (Etiquetas) y, a continuación, Create Tag (Crear etiqueta).

Para etiquetar una instancia de spot existente mediante la consola

Después de que se haya iniciado su solicitud de instancia de spot, puede agregar etiquetas a la instancia con la consola. Para obtener más información, consulte Agregar y eliminar etiquetas en un recurso individual.

AWS CLI

Etiquetar una solicitud de instancia de spot o una instancia de spot existente mediante AWS CLI

Utilice el comando create-tags para etiquetar recursos existentes. En el siguiente ejemplo, la solicitud de instancia de spot existente y la instancia de spot se etiquetan con Key=purpose y Value=test.

```
aws ec2 create-tags \
    --resources sir-08b93456 i-1234567890abcdef0 \
    --tags Key=purpose,Value=test
```

Ver las etiquetas de las solicitudes de instancias de spot

Console

Para ver etiquetas de la solicitud de instancia de spot mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Solicitudes de spot.

3. seleccione su solicitud de instancia de spot y elija la pestaña Tags (Etiquetas).

AWS CLI

Para describir las etiquetas de solicitud de instancia de spot

Las etiquetas de una solicitud de una instancia de spot se pueden ver al describir esa misma solicitud. Utilice el comando describe-spot-instance-requests para ver la configuración de la solicitud de instancia de spot especificada, que incluye las etiquetas especificadas para la solicitud.

```
aws ec2 describe-spot-instance-requests \
    --spot-instance-request-ids sir-EXAMPLE1 \
    --query "SpotInstanceRequests[*].Tags"
```

A continuación, se muestra un ejemplo del resultado.

```
[
    [
        {
            "Key": "Environment",
            "Value": "Production"
        },
        {
            "Key": "Department",
            "Value": "101"
        }
    ]
]
```

Cancelar una solicitud de instancia de spot

Si ya no quiere la solicitud de instancia de spot, puede cancelarla. Solo puede cancelar solicitudes de instancia de spot cuyo estado sea `open`, `active` o `disabled`.

- El estado de la solicitud de instancia de spot es `open` cuando aún no se ha atendido la solicitud y no se ha iniciado ninguna instancia.
- El estado de la solicitud de instancia de spot es `active` cuando se ha atendido la solicitud y, como resultado, se han iniciado dichas instancias.

- Su solicitud de instancia de spot es `disabled` cuando detiene su instancia de spot.

Si el estado de la solicitud de instancia de spot es `active` y tiene una instancia de spot asociada en ejecución, la cancelación de la solicitud no termina la instancia. Para obtener más información acerca de cómo terminar las instancias de Spot, consulte Terminar una instancia de spot.

Console

Para cancelar una solicitud de una instancia de spot a través de la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Solicitudes de spot.
3. Seleccione la solicitud de la instancia de spot.
4. Elija Acciones, Cancelar comando.
5. (Opcional) Si ha acabado con las instancias de spot asociadas, puede terminarlas. En el cuadro de diálogo Cancelar solicitud de Spot seleccione Terminar instancias, y, a continuación, elija Confirmar.

AWS CLI

Para cancelar una solicitud de una instancia de spot a través de la AWS CLI

Use el comando cancel-spot-instance-requests para cancelar la solicitud de instancia de spot especificada.

```
aws ec2 cancel-spot-instance-requests --spot-instance-request-ids sir-08b93456
```

Detener una instancia de spot

Si no necesita sus instancias de spot ahora, pero desea reiniciarlas más tarde sin perder los datos que persisten en el volumen de Amazon EBS, puede detenerlas. Los pasos que se llevan a cabo para detener una instancia de spot son similares a los pasos para detener una instancia bajo demanda.

> **Note**
>
> Mientras la instancia de spot esté detenida, puede modificar algunos de sus atributos, pero no el tipo de instancia.
> Las instancias de spot detenidas no suponen cargos de uso ni tarifas de transferencia de datos, pero sí se cobra por el almacenamiento de cualquier volumen de Amazon EBS.

Limitaciones

- Solo puede detener una instancia de spot si esta se lanzó desde una solicitud de instancia de spot `persistent`.
- No se puede detener una instancia de spot si se ha cancelado la solicitud de instancia de spot asociada. Cuando se ha cancelado la solicitud de instancia de spot, solo usted puede terminarla.
- No se puede detener una instancia de spot si forma parte de una flota, un grupo de inicialización o un grupo de zona de disponibilidad.

Console

Para detener una instancia de spot a través de la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Seleccione la instancia de spot. Si no guardó el ID de instancia de la instancia de spot, consulte the section called “Búsqueda de instancias de spot”.
4. Elija Instance state (Estado de la instancia) y Stop instance (Detener instancia).
5. Cuando se le pida que confirme, elija Stop.

AWS CLI

Para detener una instancia de spot a través de la AWS CLI

Utilice el comando stop-instances para detener de manera manual las instancias de spot.

```
aws ec2 stop-instances --instance-ids i-1234567890abcdef0
```

Iniciar una instancia de spot

Puede iniciar una instancia de spot que detuvo previamente.

Requisitos previos

Solo puede iniciar una instancia de spot en los siguientes casos:

- Detuvo la instancia de spot manualmente.
- La instancia de spot es una instancia con respaldo de EBS.
- Hay capacidad de instancia de spot disponible.
- El precio de spot es inferior al precio máximo.

Limitaciones

- No se puede iniciar una instancia de spot si forma parte de una flota, un grupo de inicialización o un grupo de zona de disponibilidad.

Los pasos que se llevan a cabo para iniciar una instancia de spot son similares a los pasos para iniciar una instancia bajo demanda.

Console

Para iniciar una instancia de spot a través de la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Seleccione la instancia de spot. Si no guardó el ID de instancia de la instancia de spot, consulte the section called “Búsqueda de instancias de spot”.
4. Elija Instance state (Estado de la instancia) y Start instance (Iniciar instancia).

AWS CLI

Para iniciar una instancia de spot a través de la AWS CLI

Utilice el comando start-instances para iniciar de manera manual las instancias de spot.

```
aws ec2 start-instances --instance-ids i-1234567890abcdef0
```

Terminar una instancia de spot

Si termina una instancia de spot en ejecución o detenida que se haya iniciado mediante una solicitud de instancia de spot persistente, esta solicitud pasará al estado `open` para que se pueda iniciar una nueva instancia de spot. Para asegurarse de que no se lance ninguna nueva instancia de spot, primero es necesario que cancele la solicitud de instancia de spot.

Si cancela una solicitud de instancia de spot `active` que tiene una instancia de spot en ejecución, esta no se termina automáticamente; por el contrario, debe terminar manualmente la instancia de spot.

Si cancela una solicitud de instancia de spot `disabled` que tiene una instancia de spot detenida, el servicio de spot de Amazon EC2 terminará automáticamente esa instancia de spot detenida. Puede haber un breve retraso entre el momento en que cancela la solicitud de instancia de spot y el momento en que el servicio de spot termina esa instancia de spot.

Para obtener más información, consulte Cancelar una solicitud de instancia de spot.

Console

Para terminar manualmente una instancia de spot mediante la consola

1. Antes de terminar la instancia, verifique que no va a perder ningún dato comprobando que los volúmenes de Amazon EBS no se eliminarán al terminar y que ha copiado los datos que necesita de los volúmenes de almacén de instancias en almacenamiento persistente, como Amazon EBS o Amazon S3.
2. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
3. En el panel de navegación, seleccione Instances (Instancia[s]).
4. Seleccione la instancia de spot. Si no guardó el ID de instancia de la instancia de spot, consulte the section called “Búsqueda de instancias de spot”.
5. Elija Instance state (Estado de la instancia) y Terminate instance (Terminar instancia).
6. Cuando se le indique que confirme, elija Terminar.

AWS CLI

Terminar manualmente una instancia de spot mediante AWS CLI

Utilice el comando terminate-instances para finalizar de manera manual las instancias de spot.

```
aws ec2 terminate-instances --instance-ids i-1234567890abcdef0 i-0598c7d356eba48d7
```

Ejemplo de especificaciones de inicialización de solicitudes de instancia de spot

En los siguientes ejemplos, se muestran configuraciones de inicialización que puede utilizar con el comando request-spot-instances (Solicitar instancias de spot) para crear una solicitud de instancia de spot. Para obtener más información, consulte Crear una solicitud de instancia de spot.

> **Important**
>
> Se desaconseja utilizar el comando request-spot-instances para solicitar una instancia de spot, ya que es una API heredada sin inversión planificada. Para obtener más información, consulte ¿Cuál es el mejor método de solicitud de spot que se puede utilizar?

Ejemplos

- Ejemplo 1: inicialización de instancias de spot
- Ejemplo 2: inicialización de instancias de spot en la zona de disponibilidad especificada
- Ejemplo 3: inicialización de instancias de spot en la subred especificada
- Ejemplo 4: inicialización de una instancia de spot dedicada

Ejemplo 1: inicialización de instancias de spot

En el siguiente ejemplo, no se incluye una zona de disponibilidad o una subred. Amazon EC2 selecciona una zona de disponibilidad para usted. Amazon EC2 inicia las instancias en la subred predeterminada de la zona de disponibilidad seleccionada.

```
{
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "m5.medium",
  "IamInstanceProfile": {
      "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

Ejemplo 2: inicialización de instancias de spot en la zona de disponibilidad especificada

En el siguiente ejemplo, se incluye una zona de disponibilidad. Amazon EC2 inicia las instancias en la subred predeterminada de la zona de disponibilidad especificada.

```
{
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "m5.medium",
  "Placement": {
    "AvailabilityZone": "us-west-2a"
  },
  "IamInstanceProfile": {
      "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

Ejemplo 3: inicialización de instancias de spot en la subred especificada

En el siguiente ejemplo, se incluye una subred. Amazon EC2 inicia las instancias en la subred especificada. Si la VPC es una VPC no predeterminada, la instancia no recibe una dirección IPv4 pública de forma predeterminada.

```
{
  "ImageId": "ami-0abcdef1234567890",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "m5.medium",
  "SubnetId": "subnet-1a2b3c4d",
  "IamInstanceProfile": {
      "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

Para asignar una dirección IPv4 pública a una instancia en una VPC no predeterminada, especifique el campo `AssociatePublicIpAddress` tal como se muestra en el siguiente ejemplo. Cuando especifica una interfaz de red, debe incluir el ID de subred y el ID de grupo de seguridad mediante la interfaz de red, en lugar de usar los campos `SubnetId` y `SecurityGroupIds` que se muestran en el bloque de código anterior.

```
{
```

```
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "InstanceType": "m5.medium",
  "NetworkInterfaces": [
    {
      "DeviceIndex": 0,
      "SubnetId": "subnet-1a2b3c4d5e6f7g8h9",
      "Groups": [ "sg-1a2b3c4d5e6f7g8h9" ],
      "AssociatePublicIpAddress": true
    }
  ],
  "IamInstanceProfile": {
      "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

Ejemplo 4: inicialización de una instancia de spot dedicada

En el siguiente ejemplo, se solicita una instancia de spot con una tenencia `dedicated`. Una instancia de spot dedicada se debe iniciar en una VPC.

```
{
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "c5.8xlarge",
  "SubnetId": "subnet-1a2b3c4d5e6f7g8h9",
  "Placement": {
    "Tenancy": "dedicated"
  }
}
```

Estado de las solicitudes de spot

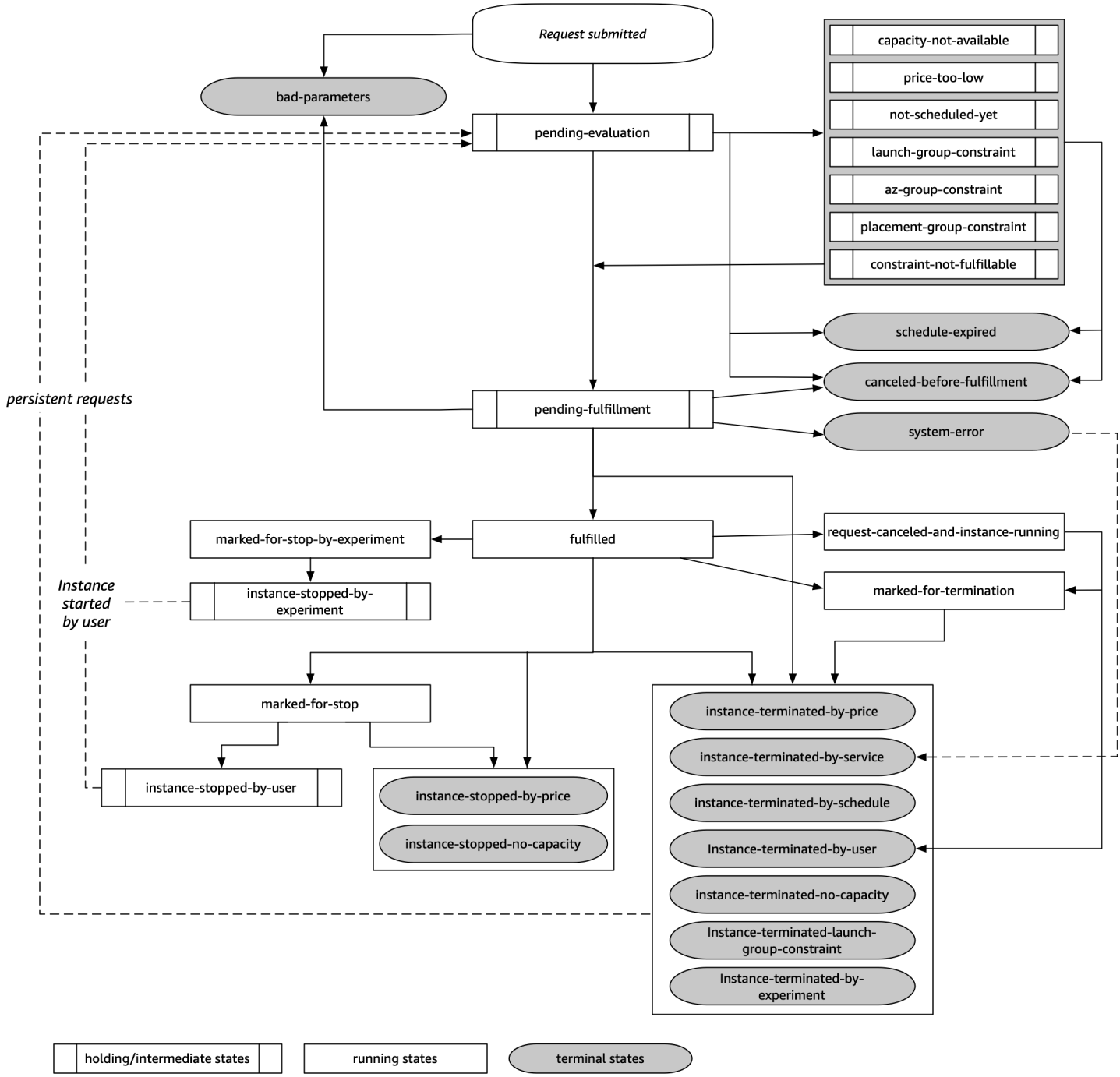
Para ayudarlo a realizar el seguimiento de sus solicitudes de instancia de spot y planificar el uso de instancias spot, utilice el estado de solicitud proporcionado por Amazon EC2. Por ejemplo, el estado de las solicitudes puede indicar la razón por la que su solicitud de spot aún no ha sido atendida, o enumerar las restricciones que están impidiendo que se atienda.

En cada paso del proceso —también denominado ciclo de vida— de la solicitud de spot, eventos específicos determinan los sucesivos estados de la solicitud.

Contenido

Ciclo de vida de una solicitud de spot

En el siguiente diagrama se muestran las rutas que su solicitud de spot puede seguir a lo largo de todo su ciclo de vida, desde el envío hasta su terminación. Cada paso aparece representado como un nodo y el código de estado de cada nodo describe el estado de la solicitud de Spot y de la instancia de Spot.



Pending evaluation

En cuanto se crea una solicitud de instancia de spot, esta pasa al estado `pending-evaluation`, a menos que haya uno o varios parámetros de la solicitud que no sean válidos (`bad-parameters`).

Código de estado	Estado de la solicitud	Estado de la instancia
`pending-evaluation`	`open`	No aplicable
`bad-parameters`	`closed`	No aplicable

Holding

Si una o varias restricciones de la solicitud son válidas pero aún no se pueden satisfacer, o si no hay suficiente capacidad, la solicitud pasa a un estado de retención en espera de que se satisfagan las restricciones. Las opciones de la solicitud afectan a la probabilidad de que se atienda la solicitud. Por ejemplo, si no hay capacidad, la solicitud permanecerá en estado de retención hasta que haya capacidad disponible. Si especifica un grupo de zona de disponibilidad, la solicitud permanece en un estado de retención hasta que se satisfaga la restricción de la zona de disponibilidad.

En el caso de interrupción del servicio de una de las zonas de disponibilidad, existe la posibilidad de que se pueda ver afectada la capacidad de EC2 que no se utiliza disponible para solicitudes de instancia de spot en otras zonas de disponibilidad.

Código de estado	Estado de la solicitud	Estado de la instancia
`capacity-not-available`	`open`	No aplicable
`price-too-low`	`open`	No aplicable
`not-scheduled-yet`	`open`	No aplicable
`launch-group-constraint`	`open`	No aplicable
`az-group-constraint`	`open`	No aplicable
`placement-group-constraint`	`open`	No aplicable

Código de estado	Estado de la solicitud	Estado de la instancia
`constraint-not-fulfillable`	`open`	No aplicable

Pending evaluation/fulfillment-terminal

La solicitud de instancia de spot puede pasar a un estado `terminal` si crea una solicitud que solo es válida durante un periodo de tiempo específico y dicho periodo caduca antes de que la solicitud alcance la fase de cumplimiento pendiente. También puede ocurrir si cancela la solicitud o si se produce un error del sistema.

Código de estado	Estado de la solicitud	Estado de la instancia
`schedule-expired`	`cancelled`	No aplicable
`canceled-before-fulfillment` [1]	`cancelled`	No aplicable
`bad-parameters`	`failed`	No aplicable
`system-error`	`closed`	No aplicable

[1] Si cancela la solicitud.

Pending fulfillment

Cuando se cumplen las restricciones que especificó (de haberlas), la solicitud de spot pasa al estado `pending-fulfillment` (pendiente de completarse).

En este punto, Amazon EC2 se está preparando para aprovisionar las instancias que solicitó. Si el proceso se detiene a esta altura, es bastante probable que se deba a que lo canceló el usuario antes de que se iniciara una instancia de spot. También puede deberse a un error inesperado del sistema.

Código de estado	Estado de la solicitud	Estado de la instancia
`pending-fulfillment`	`open`	No aplicable

Fulfilled

Cuando se cumplen todas las especificaciones de las instancias de spot, su solicitud de spot se habrá atendido. Amazon EC2 inicia las instancias de spot, lo que puede tardar unos minutos. Si una instancia de spot hiberna o se detiene con la interrupción, permanece en este estado hasta que la solicitud se pueda atender de nuevo o se cancele.

Código de estado	Estado de la solicitud	El estado de la instancia
`fulfilled`	`active`	`pending` → `running`
`fulfilled`	`active`	`stopped` → `running`

Si detiene una instancia de spot, su solicitud de spot entrará en el estado `marked-for-stop` o `instance-stopped-by-user` hasta que la instancia de spot se pueda iniciar de nuevo o se cancele la solicitud.

Código de estado	Estado de la solicitud	El estado de la instancia
`marked-for-stop`	`active`	`stopping`
`instance-stopped-by-user` [1]	`disabled` o `cancelled` [2]	`stopped`

[1] Una instancia de spot entra en el estado `instance-stopped-by-user` si detiene la instancia o ejecuta el comando “shutdown” (Apagado), desde la instancia. Una vez que haya detenido la instancia, puede iniciarla de nuevo. Al reiniciar, la solicitud de instancia de spot vuelve al estado `pending-evaluation` y, a continuación, Amazon EC2 inicia una nueva instancia de spot cuando se cumplen las restricciones.

² El estado de la solicitud de spot es `disabled` si detiene la instancia de spot, pero no cancela la solicitud. El estado de la solicitud es `cancelled` si la instancia de spot se detiene y la solicitud caduca.

Fulfilled-terminal

Las instancias de spot continúan ejecutándose mientras haya capacidad de spot disponible para su tipo de instancia y usted no las termine. Si Amazon EC2 debe terminar las instancias de spot, la solicitud de spot pasa a un estado terminal. Una solicitud también pasa al estado terminal si se cancela la solicitud de instancia de spot o se terminan las instancias de spot.

Código de estado	Estado de la solicitud	El estado de la instancia
`request-canceled-and-instance-running`	`cancelled`	`running`
`marked-for-stop`	`active`	`running`
`marked-for-termination`	`active`	`running`
`instance-stopped-by-price`	`disabled`	`stopped`
`instance-stopped-by-user`	`disabled`	`stopped`
`instance-stopped-no-capacity`	`disabled`	`stopped`
`instance-terminated-by-price`	`closed` (una única vez), `open` (persistente)	`terminated`
`instance-terminated-by-schedule`	`closed`	`terminated`
`instance-terminated-by-service`	`cancelled`	`terminated`

Código de estado	Estado de la solicitud	El estado de la instancia
`instance-terminated-by-user`	`closed` o `cancelled` [1]	`terminated`
`instance-terminated-no-capacity`	`closed` (una única vez), `open` (persistente)	`running` †
`instance-terminated-no-capacity`	`closed` (una única vez), `open` (persistente)	`terminated`
`instance-terminated-launch-group-constraint`	`closed` (una única vez), `open` (persistente)	`terminated`

[1] El estado de la solicitud es `closed` si termina la instancia pero no cancela la solicitud. El estado de la solicitud es `cancelled` si termina la instancia y cancela la solicitud. Incluso si termina una instancia de spot antes de cancelar su solicitud, podría transcurrir tiempo hasta que Amazon EC2 detecte que se ha terminado la instancia de spot. En este caso, el estado de la solicitud podría ser `closed` o `cancelled`.

† Cuando Amazon EC2 interrumpe una instancia de spot, si necesita recuperar la capacidad y la instancia está configurada para terminar en caso de interrupción, el estado se establece de forma inmediata en `instance-terminated-no-capacity` (no se establece en `marked-for-termination`). Sin embargo, la instancia permanece en estado `running` durante 2 minutos para reflejar el periodo de 2 minutos en el que la instancia recibe el aviso de interrupción de la instancia de spot. Después de 2 minutos, el estado de la instancia se establece en `terminated`.

Experimentos de interrupción

Puede utilizar AWS Fault Injection Service para iniciar la interrupción de una instancia de spot y probar la manera en que responden las aplicaciones en las instancias de spot. Si AWS FIS detiene una instancia de spot, la solicitud de spot pasará al estado `marked-for-stop-by-experiment` y luego a `instance-stopped-by-experiment`. Si AWS FIS finaliza una instancia de spot, la solicitud de spot pasará al estado `instance-terminated-by-experiment`. Para obtener más información, consulte the section called “Iniciar una interrupción”.

Código de estado	Estado de la solicitud	El estado de la instancia
`marked-for-stop-by-experiment`	`active`	`running`
`instance-stopped-by-experiment`	`disabled`	`stopped`
`instance-terminated-by-experiment`	`closed`	`terminated`

Solicitudes persistentes

Cuando usted o Amazon EC2; terminan las instancias de spot, si la solicitud de spot es persistente, esta regresa al estado `pending-evaluation` y entonces Amazon EC2 podrá iniciar una nueva instancia de spot cuando se cumplan las restricciones.

Obtener información del estado de la solicitud

Se puede obtener información de estado de las solicitudes mediante la AWS Management Console o una herramienta de línea de comandos.

Para ver la información del estado de la solicitud a través de la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Spot Requests (Solicitudes de spot) y, a continuación, seleccione la solicitud de spot.
3. Para comprobar el estado, en la pestaña Descripción, compruebe el campo Estado.

Para obtener información de estado de las solicitudes 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 Acceder a Amazon EC2.

- describe-spot-instance-requests (AWS CLI)
- Get-EC2SpotInstanceRequest (AWS Tools for Windows PowerShell)

Códigos de estado de las solicitudes de spot

La información de estado de las solicitudes de spot se compone de un código de estado de puja, la hora de la actualización y un mensaje de estado. Juntos, ayudan a determinar la disposición de su solicitud de spot.

A continuación se enumeran los códigos de estado de las solicitudes de spot:

`az-group-constraint`

Amazon EC2 no puede iniciar todas las instancias que solicitó en la misma zona de disponibilidad.

`bad-parameters`

Uno o varios parámetros de su solicitud de spot no son válidos (por ejemplo, la AMI que especificó no existe). El mensaje de estado indica cuál es el parámetro que no es válido.

`canceled-before-fulfillment`

El usuario canceló la solicitud de spot antes de que se atendiera.

`capacity-not-available`

No hay suficiente capacidad disponible para las instancias que ha solicitado.

`constraint-not-fulfillable`

No se puede atender la solicitud de spot porque una o varias restricciones no son válidas (por ejemplo, la zona de disponibilidad no existe). El mensaje de estado indica cuál es la restricción que no es válida.

`fulfilled`

La solicitud de spot es `active` y Amazon EC2 está iniciando su instancias de spot.

`instance-stopped-by-price`

La instancia se ha detenido porque el precio de spot ha superado el precio máximo.

`instance-stopped-by-user`

La instancia se detuvo porque un usuario detuvo la instancia o ejecutó el comando shutdown desde la instancia.

`instance-stopped-no-capacity`

Su instancia se detuvo debido a las necesidades de administración de capacidad de EC2.

`instance-terminated-by-price`

La instancia se ha terminado porque el precio de spot ha superado el precio máximo. Si su solicitud es persistente, el proceso se reinicia, por lo que la solicitud está pendiente de evaluación.

`instance-terminated-by-schedule`

La instancia de spot se terminó al final de la duración programada.

`instance-terminated-by-service`

Su instancia se terminó desde un estado detenido.

`instance-terminated-by-user` o `spot-instance-terminated-by-user`

Ha terminado una instancia de spot que había sido atendida, por lo que el estado de la solicitud es `closed` (a menos que sea una solicitud persistente) y el estado de la instancia es `terminated`.

`instance-terminated-launch-group-constraint`

Se han terminado una o varias instancias en su grupo de inicialización, por lo que la restricción del grupo de inicialización ya no se cumple.

`instance-terminated-no-capacity`

Su instancia se terminó debido a los procesos de administración de capacidad estándar.

`launch-group-constraint`

Amazon EC2 no puede iniciar todas las instancias que solicitó al mismo tiempo. Todas las instancias en un grupo de inicialización se inician y se terminan juntas.

`limit-exceeded`

Se ha excedido el límite en el número de volúmenes de EBS o en el almacenamiento de volumen total. Para obtener más información sobre estos límites y sobre cómo solicitar un incremento, consulte Límites de Amazon EBS en Referencia general de Amazon Web Services.

`marked-for-stop`

La instancia de spot está marcada para su detención.

`marked-for-termination`

La instancia de spot está marcada para su terminación.

`not-scheduled-yet`

La solicitud de spot no se evaluará hasta la fecha programada.

`pending-evaluation`

Después de realizar una solicitud de instancia de spot, esta pasa al estado `pending-evaluation` mientras el sistema evalúa los parámetros de la solicitud.

`pending-fulfillment`

Amazon EC2 está intentando aprovisionar las instancias de spot.

`placement-group-constraint`

Aún no se puede atender la solicitud de spot porque, en este momento, no se puede agregar una instancia de spot al grupo de ubicación.

`price-too-low`

Aún no se puede atender la solicitud porque el precio máximo está por debajo del precio de spot. En este caso, no se inicia ninguna instancia y su solicitud permanece en estado `open`.

`request-canceled-and-instance-running`

Usted canceló la solicitud de spot mientras las instancias de spot aún estaban en ejecución. El estado de la solicitud es `cancelled`, pero las instancias tienen el estado `running`.

`schedule-expired`

La solicitud de spot caducó porque no se atendió antes de la fecha especificada.

`system-error`

Se ha producido un error inesperado del sistema. Si es un problema recurrente, contacte con AWS Support para obtener ayuda.

Evento de cumplimiento de solicitud de instancia de spot de EC2

Cuando se cumple una solicitud de instancia de spot, Amazon EC2 envía un evento de cumplimiento de solicitud de instancia de spot de EC2 a Amazon EventBridge. Puede crear una regla para realizar una acción cada vez que se produzca este evento, como invocar una función de Lambda o notificar un tema de Amazon SNS.

El siguiente es un ejemplo de los datos de este evento.

```
{
    "version": "0",
    "id": "01234567-1234-0123-1234-012345678901",
    "detail-type": "EC2 Spot Instance Request Fulfillment",
    "source": "aws.ec2",
    "account": "123456789012",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-2",
    "resources": ["arn:aws:ec2:us-east-2:123456789012:instance/i-1234567890abcdef0"],
    "detail": {
        "spot-instance-request-id": "sir-1a2b3c4d",
        "instance-id": "i-1234567890abcdef0"
    }
}
```

Para más información, consulte la Guía del usuario de Amazon EventBridge.

Recomendación de reequilibrio de instancias de EC2

Una recomendación de reequilibrio de instancia de EC2 es una señal que notifica cuando una instancia de spot corre riesgo elevado de interrupción. La señal puede llegar antes del aviso de interrupción de instancia de spot de dos minutos, lo que brinda la oportunidad de administrar proactivamente la instancia de spot. Puede decidir reequilibrar su carga de trabajo con instancias de spot nuevos o existentes que no tengan un riesgo elevado de interrupción.

Amazon EC2 no siempre puede enviar la señal de recomendación de reequilibrio antes del aviso de interrupción de dos minutos de instancia de spot. Por lo tanto, la señal de recomendación de reequilibrio puede llegar junto con el aviso de interrupción de dos minutos.

Las recomendaciones de reequilibrio están disponibles como CloudWatch Events y como elementos en los metadatos de instancia en la instancia de spot. Los eventos se emiten en la medida de lo posible.

> **Note**
>
> Las recomendaciones de reequilibrio solo se admiten para instancias de spot que se inician después del 5 de noviembre de 2020 a las 00:00 UTC.

Temas

Reequilibrar las acciones que puede realizar

Estas son algunas de las posibles acciones de reequilibrio que puede realizar:

Apagado correcto

Cuando reciba la señal de recomendación de reequilibrio para una instancia de spot, puede comenzar los procedimientos de apagado de la instancia, los cuales pueden incluir asegurarse de que los procesos se completen antes de detenerlos. Por ejemplo, puede cargar registros del sistema o de aplicaciones en Amazon Simple Storage Service (Amazon S3), cerrar los trabajadores de Amazon SQS o completar la anulación del registro desde el sistema de nombres de dominio (DNS). También puede guardar su trabajo en almacenamiento externo y reanudarlo más adelante.

Evitar que se programe un nuevo trabajo

Cuando reciba la señal de recomendación de reequilibrio para una instancia de spot, puede evitar que se programe trabajo nuevo en la instancia, a la vez que continúa utilizando la instancia hasta que se complete el trabajo programado.

iniciar de forma proactiva nuevas instancias de reemplazo

Puede configurar grupos de escalado automático, flotas de EC2 o flotas de spot para iniciar automáticamente las instancias de spot de reemplazo cuando se emite una señal de recomendación de reequilibrio. Para obtener más información, consulte Utilizar el reequilibrio de capacidad para gestionar las interrupciones de spot de Amazon EC2 en la Guía del usuario de Amazon EC2 Auto Scaling y Reequilibrio de la capacidad para la flota de EC2 y Reequilibrio de la capacidad para la flota de spot, en esta guía del usuario.

Monitorear las señales de recomendación de reequilibrio

Puede monitorear la señal de recomendación de reequilibrio para que, cuando se emita, pueda realizar las acciones especificadas en la sección anterior. La señal de recomendación de reequilibrio está disponible como un evento que se envía a Amazon EventBridge (antes conocido como Amazon CloudWatch Events) y como metadatos de instancia en la instancia de spot.

Monitorear las señales de recomendación de reequilibrio:

- Usar Amazon EventBridge
- Usar metadatos de instancia

Usar Amazon EventBridge

Cuando se emite la señal de recomendación de reequilibrio para una instancia de spot, el evento de la señal se envía a Amazon EventBridge. Si EventBridge detecta un patrón de eventos que coincide con un patrón definido en una regla, EventBridge invoca un destino (o destinos) especificados en la regla.

El siguiente es un evento de ejemplo para la señal de recomendación de reequilibrio.

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-123456789012",
    "detail-type": "EC2 Instance Rebalance Recommendation",
    "source": "aws.ec2",
    "account": "123456789012",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-2",
    "resources": ["arn:aws:ec2:us-east-2:123456789012:instance/i-1234567890abcdef0"],
    "detail": {
        "instance-id": "i-1234567890abcdef0"
    }
}
```

Los siguientes campos forman el patrón de eventos definido en la regla:

`"detail-type": "EC2 Instance Rebalance Recommendation"`

Identifica que el evento es un evento de recomendación de reequilibrio

`"source": "aws.ec2"`

Identifica que el evento es de Amazon EC2.

Crear una regla de EventBridge

Puede escribir una regla de EventBridge y automatizar qué acciones tomar cuando el patrón de eventos coincida con la regla.

En el ejemplo siguiente se crea una regla de EventBridge para enviar un correo electrónico, un mensaje de texto o una notificación push móvil cada vez que Amazon EC2 emite una señal de recomendación de reequilibrio. La señal se emite como un evento de `EC2 Instance Rebalance Recommendation`, lo que desencadena la acción definida por la regla.

Antes de crear la regla de EventBridge, debe crear el tema de Amazon SNS para el email, el mensaje de texto o la notificación push móvil.

Para crear una regla de EventBridge para un evento de recomendación de reequilibrio

1. Abra la consola de Amazon EventBridge en https://console.aws.amazon.com/events/.
2. Elija Crear regla.
3. En Definir detalle de la regla, haga lo siguiente:
   a. Ingrese un Nombre para la regla y, opcionalmente, una descripción.

      Una regla no puede tener el mismo nombre que otra regla de la misma región y del mismo bus de eventos.
   b. En Bus de eventos, elija Predeterminado. Cuando un servicio de AWS en su cuenta emite un evento, siempre se dirige al bus de eventos predeterminado de su cuenta.
   c. En Tipo de regla, elija Regla con un patrón de evento.
   d. Elija Siguiente.
4. En Crear patrón de evento, realice una de las siguientes acciones:
   a. En Origen del evento, elija Eventos o eventos de socios de EventBridge de AWS.
   b. En Event pattern (Patrón de eventos), en este ejemplo, especificará el siguiente patrón de eventos para que coincida con el evento `EC2 Instance Rebalance Recommendation` y, a continuación, elija Save (Guardar).

      ```
      {
       "source": ["aws.ec2"],
       "detail-type": ["EC2 Instance Rebalance Recommendation"]
      }
      ```

      Para agregar el patrón de evento, puede utilizar una plantilla por medio de la opción Formulario de patrón de evento o puede especificar su propio patrón por medio de la opción Patrón personalizado (editor de JSON), de la siguiente manera:

i. Para utilizar una plantilla con el objetivo de crear el patrón de evento, haga lo siguiente:

A. Seleccione Formulario de patrón de evento.

B. En Origen del evento, elija Servicios de AWS.

C. En Servicio de AWS, elija Flota de spot de EC2.

D. En Tipo de evento, elija Recomendación de reequilibrio de las instancias de EC2.

E. Para personalizar la plantilla, elija Editar patrón y realice los cambios para que coincidan con el patrón de evento de ejemplo.

ii. (Alternativa) Para especificar un patrón de evento personalizado, haga lo siguiente:

A. Elija Custom pattern (JSON editor) (Patrón personalizado [editor de JSON]).

B. En el casillero Patrón de evento, agregue el patrón de eventos de este ejemplo.

c. Elija Siguiente.

5. En Seleccionar destino, realice una de las siguientes acciones:

a. En Tipos de destino, elija Servicio de AWS.

b. En Seleccionar un destino, elija Tema de SNS para enviar un email, un mensaje de texto o una notificación push móvil cuando se produzca el evento.

c. En Tema, elija un tema existente. Primero debe crear un tema de Amazon SNS mediante la consola de Amazon SNS. A fin de obtener más información, consulte Uso de Amazon SNS para mensajería de aplicación a persona (A2P) en Guía para desarrolladores de Amazon Simple Notification Service.

d. (Opcional) En Configuración adicional, puede configurar opciones adicionales. Para obtener más información, consulte Creación de reglas de EventBridge que reaccionan a eventos (paso 16) en la Guía del usuario de Amazon EventBridge.

e. Elija Siguiente.

6. (Opcional) En Etiquetas, puede asignar una o varias etiquetas a la regla y, a continuación, elija Siguiente.

7. En Revisar y crear, realice una de las siguientes acciones:

a. Revise los detalles de la regla y modifíquelos según sea necesario.

b. Elija Crear regla.

Para obtener más información, consulte Reglas de Amazon EventBridge y Patrones de eventos de Amazon EventBridge en la Guía del usuario de Amazon EventBridge.

Usar metadatos de instancia

La categoría de metadatos de instancia `events/recommendations/rebalance` proporciona el tiempo aproximado, en UTC, cuando se emitió la señal de recomendación de reequilibrio para una instancia de spot.

Recomendamos que compruebe si hay señales de recomendación de reequilibrio cada 5 segundos para que no pierda la oportunidad de actuar en función de la recomendación de reequilibrio.

Si una instancia de spot recibe una recomendación de reequilibrio, la hora en que se emitió la señal está presente en los metadatos de la instancia. Puede recuperar la hora en que se emitió la señal de la siguiente manera.

Utilice el comando correspondiente a su sistema operativo.

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/events/recommendations/rebalance
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/events/recommendations/rebalance
```

Windows

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/events/recommendations/rebalance
```

A continuación, se muestra un ejemplo de salida, que indica la hora, en UTC, a la que se emitió la señal de recomendación de reequilibrio para la instancia de spot.

```
{"noticeTime": "2020-10-27T08:22:00Z"}
```

Si la señal no se ha emitido para la instancia, la `events/recommendations/rebalance` no está presente y recibirá un error HTTP 404 cuando intente recuperarla.

Servicios que utilizan la señal de recomendación de reequilibrio

Amazon EC2 Auto Scaling, la flota de EC2 y la flota de spot utilizan la señal de recomendación de reequilibrio para facilitar el mantenimiento de la disponibilidad de la carga de trabajo mediante el aumento proactivo de su flota con una nueva instancia de spot antes de que una instancia en ejecución reciba el aviso de interrupción de instancia de spot de dos minutos. Puede hacer que estos servicios monitoreen y respondan de forma proactiva a los cambios que afectan a la disponibilidad de su instancias de spot. Para más información, consulte los siguientes temas:

- Utilizar el reequilibrio de capacidad para gestionar las interrupciones de spot de Amazon EC2 en la Guía del usuario de Amazon EC2 Auto Scaling
- Reequilibrio de la capacidad en el tema de flota de EC2 de esta guía del usuario
- Reequilibrio de la capacidad en el tema flota de spot de esta guía del usuario

Interrupciones de instancias de spot

Puede iniciar instancias de spot con capacidad de EC2 extra para disfrutar de importantes descuentos a cambio de devolverlos cuando Amazon EC2 necesite de nuevo esa capacidad. Cuando Amazon EC2 recupera una instancia de spot, llamamos a este evento interrupción de una instancia de spot.

Cuando Amazon EC2 interrumpe una instancia de spot, termina, detiene o hiberna la instancia, según lo que especificó cuando creó la solicitud de spot.

La demanda de instancias de spot puede variar enormemente de un momento a otro, y la disponibilidad de las instancias de spot también puede variar significativamente en función de cuántas instancias de EC2 no utilizadas haya disponibles. Siempre es posible que la instancia de spot se vea interrumpida.

Una instancia bajo demanda especificada en una flota de EC2 o una flota de spot no se puede interrumpir.

Contenido

Razones para la interrupción de una instancia de spot

A continuación se enumeran las posibles razones por las que Amazon EC2 puede interrumpir las instancias de spot.

Capacidad

Amazon EC2 puede interrumpir su instancia de spot cuando vuelve a necesitarla. EC2 recupera la instancia principalmente para reutilizar la capacidad, pero también puede ocurrir por otras razones, como mantenimiento del host o desmantelamiento del equipo.

Precio

El precio de spot es superior al precio máximo.

Puede especificar el precio máximo en su solicitud de spot. Sin embargo, si especifica un precio máximo, las instancias se interrumpirán con más frecuencia que si no lo elige.

Restricciones

Si la solicitud de spot incluye una restricción, como un grupo de inicialización o un grupo de zona de disponibilidad, estas instancias de spot se terminan como grupo cuando ya no se puede cumplir la restricción.

Puede ver las tasas de interrupción históricas de su tipo de instancias en el Asistente de instancias de spot.

Comportamiento de las interrupciones de las instancias de spot

Puede especificar que Amazon EC2 debe realizar una de las siguientes acciones cuando interrumpa una instancia de spot:

- Detener instancias de spot interrumpida
- Hibernar instancias de spot interrumpida
- Terminar instancias de spot interrumpidas (este es el comportamiento predeterminado)

Especificar el comportamiento de interrupción

Puede especificar el comportamiento de la interrupción al crear una solicitud de spot. Si no especifica un comportamiento de la interrupción, Amazon EC2 terminará instancias de spot de forma predeterminada cuando se produzca la interrupción.

La forma en que se especifica el comportamiento de la interrupción depende de la forma en la que solicite instancias de spot.

- Si solicita instancias de spot en un asistente de inicialización de instancias, puede especificar el comportamiento de la interrupción de la siguiente manera: en el asistente de inicialización de instancias, expanda Detalles avanzados y seleccione la casilla de verificación Solicitar instancias de spot. Elija Personalizar. En Comportamiento de interrupción, seleccione un comportamiento de interrupción. Si el comportamiento de interrupción es la hibernación, también puede seleccionar Habilitar para Detener: comportamiento de hibernación.
- Si solicita instancias de spot mediante la CLI run-instances, puede especificar el comportamiento de interrupción de la siguiente manera: en la configuración de la solicitud, (`--instance-market-options`), en `InstanceInterruptionBehavior`, especifique un comportamiento de interrupción. Si el comportamiento de interrupción es `hibernate`, también puede habilitar la hibernación mediante el parámetro `--hibernation-options Configured=true`.
- Si configura instancias de spot en una plantilla de inicialización, puede especificar el comportamiento de la interrupción de la siguiente manera: en la plantilla de inicialización, expanda Detalles avanzados y seleccione la casilla de verificación Solicitar instancias de spot. Elija Personalizar y, a continuación, en Comportamiento de interrupción, seleccione un comportamiento de la interrupción.
- Si solicita instancias de spot mediante la consola de spot, puede especificar el comportamiento de la interrupción de la siguiente manera: active la casilla de verificación Mantener capacidad de

destino y, a continuación, en Comportamiento de interrupción, seleccione un comportamiento de la interrupción.

- Si establece instancias de spot en una configuración de solicitud cuando utiliza la CLI create-fleet, puede especificar el comportamiento de la interrupción de la siguiente manera: en `InstanceInterruptionBehavior`, especifique un comportamiento de interrupción.
- Si establece instancias de spot en una configuración de solicitud cuando utiliza la CLI request-spot-fleet, puede especificar el comportamiento de la interrupción de la siguiente manera: en `InstanceInterruptionBehavior`, especifique un comportamiento de interrupción.
- Si configura instancias de spot mediante la CLI request-spot-instances, puede especificar el comportamiento de la interrupción de la siguiente manera: para `--instance-interruption-behavior`, especifique un comportamiento de la interrupción.

> **Note**
>
> Se desaconseja utilizar los comandos request-spot-fleet y request-spot-instances para solicitar instancias de spot, ya que son API heredadas sin inversión planificada. Para obtener más información, consulte ¿Cuál es el mejor método de solicitud de spot que se puede utilizar?

Detener instancias de spot interrumpida

Puede especificar que Amazon EC2 detenga las instancias de spot cuando se interrumpen. Para obtener más información, consulte Especificar el comportamiento de interrupción.

Consideraciones

- Solo Amazon EC2 puede reiniciar una instancia de spot interrumpida detenida.
- Para una instancia de spot iniciada por una solicitud de instancia de spot `persistent`, Amazon EC2 reinicia la instancia detenida cuando hay capacidad disponible en la misma zona de disponibilidad para el mismo tipo de instancia que la instancia detenida (se debe utilizar la misma especificación de inicialización).
- Para instancias de spot iniciadas por una flota de EC2 o una flota de spot de tipo `maintain`: después de interrumpir una instancia de spot, Amazon EC2 inicia una instancia de sustitución para mantener la capacidad de destino. Amazon EC2 busca los mejores grupos de capacidad de spot en función de la estrategia de asignación especificada (`lowestPrice`, `diversified`

o `InstancePoolsToUseCount`); no da prioridad al grupo con las instancias que se detuvieron primero. Posteriormente, si la estrategia de asignación identifica un grupo que contiene las instancias que se detuvieron primero, Amazon EC2 reinicia las instancias detenidas para mantener la capacidad de destino.

Por ejemplo, imagine una flota de spot con la estrategia de reparto `lowestPrice`. Durante la inicialización inicial, un grupo de `c3.large` satisface los criterios de `lowestPrice` de la especificación de inicialización. Más tarde, cuando las instancias `c3.large` se interrumpen, Amazon EC2 detiene las instancias y reaprovisiona la capacidad desde otro grupo que encaja con la estrategia `lowestPrice`. Esta vez, el grupo resulta ser un grupo `c4.large` y Amazon EC2 inicia instancias `c4.large` para satisfacer la capacidad de destino. Asimismo, la flota de spot no podrá cambiar a un grupo `c5.large` la próxima vez. En cada una de estas transiciones, Amazon EC2 no da prioridad a los grupos que contienen instancias que se detuvieron primero; simplemente se basa en la estrategia de asignación especificada. La estrategia `lowestPrice` puede provocar que se utilicen grupos con instancias que se detuvieron antes. Por ejemplo, si se interrumpen instancias del grupo `c5.large` y la estrategia `lowestPrice` conduce nuevamente a los grupos `c3.large` o `c4.large`, las instancias que se detuvieron se reinician hasta satisfacer la capacidad de destino.

- Mientras la instancia de spot esté detenida, puede modificar algunos de sus atributos, pero no el tipo de instancia. Si desconecta o elimina un volumen de EBS, este no estará conectado cuando se inicie la instancia de spot. Si desconecta el volumen raíz y Amazon EC2 intenta iniciar la instancia de spot, la instancia no se iniciará y Amazon EC2 terminará la instancia detenida.
- Puede terminar una instancia de spot mientras está detenida.
- Si cancela una solicitud de instancia de spot, una flota de EC2 o una flota de spot, Amazon EC2 termina todas las instancias de spot asociadas que se hayan detenido.
- Mientras una instancia de spot interrumpida está detenida, solo se le cobran los volúmenes de EBS, los cuales se conservan. Con la flota de EC2 y la flota de spot, si tiene muchas instancias detenidas, puede superar el límite de la cantidad de volúmenes de EBS de su cuenta. Para obtener más información acerca de cómo se le cobran cuando una instancia de spot se interrumpe, consulte Facturación de las instancias de spot interrumpidas.
- Asegúrese de estar familiarizado con las implicaciones de detener una instancia. Para obtener más información acerca de qué sucede cuando una instancia está detenida, consulte Diferencias entre reinicio, detención, hibernación y terminación.

Requisitos previos

Para detener una instancia de spot detenida, deben existir los requisitos previos siguientes:

Tipo de solicitud de spot

El tipo de solicitud de instancia de spot: debe ser `persistent`. No puede especificar un grupo de inicialización en la solicitud de instancia de spot.

El tipo de solicitud de flota de EC2 o flota de spot: debe ser `maintain`.

Tipo de volumen raíz

Debe ser un volumen de EBS, no un volumen de almacén de instancias.

Hibernar instancias de spot interrumpida

Puede especificar que Amazon EC2 hiberne las instancias de spot cuando se interrumpen. Para obtener más información, consulte Hibernación de la instancia de Amazon EC2.

Amazon EC2 ofrece ahora la misma experiencia de hibernación para las instancias de spot que está disponible actualmente para las instancias bajo demanda. Ofrece un soporte más amplio y ahora se admite lo siguiente para la hibernación de instancias de spot:

- Más AMI compatibles
- Más familias de instancias compatibles
- Hibernación iniciada por el usuario

Terminar instancias de spot interrumpidas

Cuando Amazon EC2 interrumpe una instancia de spot, termina la instancia de forma predeterminada, a menos que especifique un comportamiento de interrupción diferente, como detener o hibernar. Para obtener más información, consulte Especificar el comportamiento de interrupción.

Preparación para las interrupciones de las instancias de spot

La demanda de instancias de spot puede variar enormemente de un momento a otro, y la disponibilidad de las instancias de spot también puede variar significativamente en función de

cuántas instancias de EC2 no utilizadas haya disponibles. Siempre es posible que la instancia de spot se vea interrumpida. Por lo tanto, debe asegurarse de que su aplicación esté preparada para una interrupción de las instancias de Spot.

Recomendamos que siga estas prácticas recomendadas para estar preparado ante una interrupción de una instancia de spot.

- Cree la solicitud de spot con un grupo de Auto Scaling. Si se interrumpen sus instancias de spot, el grupo de Auto Scaling iniciará automáticamente instancias de reemplazo. Para obtener más información, consulte la sección sobre Grupos de escalado automático con varios tipos de instancia y opciones de compra en la guía del usuario de Amazon EC2 Auto Scaling.
- Asegúrese de que su instancia está lista para ejecutarse en cuanto se atienda la solicitud usando una Imagen de máquina de Amazon (AMI) que contiene la configuración de software requerida También puede utilizar datos de usuario para ejecutar comandos al iniciarla.
- Los datos almacenados en volúmenes de almacén de instancias se perderán cuando se detenga o termine la instancia. Haga una copia de seguridad de los datos importantes de los volúmenes de almacén de instancias en un almacenamiento más persistente, como Amazon S3, Amazon EBS o Amazon DynamoDB.
- Almacene los datos importantes periódicamente en un lugar que no se vea afectado si se termina la instancia de spot. Por ejemplo, puede utilizar Amazon S3, Amazon EBS o DynamoDB.
- Divida el trabajo en pequeñas tareas (mediante Grid, Hadoop o una arquitectura basada en colas), o use puntos de comprobación de forma que pueda grabar su trabajo con frecuencia.
- Amazon EC2 envía una señal de recomendación de reequilibrio a la instancia de spot cuando la instancia corre riesgo elevado de interrupción. Puede confiar en la recomendación de reequilibrio para administrar de forma proactiva las interrupciones de instancias de spot sin tener que esperar el aviso de interrupción de instancias de spot de dos minutos. Para obtener más información, consulte Recomendación de reequilibrio de instancias de EC2.
- Use los avisos de interrupción de instancias de spot de dos minutos para monitorear el estado de sus instancias de spot. Para obtener más información, consulte Avisos de interrupción de instancias de spot..
- Si bien hacemos todo lo posible para proporcionar estas advertencias lo antes posible, es posible que su instancia de spot se interrumpa antes de que las advertencias estén disponibles. Pruebe la aplicación para asegurarse de que maneja correctamente una interrupción de instancia inesperada, incluso si monitorea las señales de recomendación de reequilibrio y avisos de interrupción. Para hacerlo, puede ejecutar la aplicación con una instancia bajo demanda y, a continuación, forzar la terminación de la instancia bajo demanda usted mismo.

- Ejecute un experimento de inyección de errores controlado con AWS Fault Injection Service para probar cómo responde la aplicación cuando la instancia de spot se interrumpe. Para obtener más información, consulte Tutorial: Test Spot Instance interruptions using AWS FIS en la Guía del usuario de AWS Fault Injection Service.

Inicio de una interrupción de instancias de spot

Puede seleccionar una solicitud de instancia de spot o una solicitud de flota de spot en la consola de Amazon EC2 e iniciar una interrupción de instancia de spot para probar cómo las aplicaciones de sus instancias de spot gestionan las interrupciones. Cuando inicia una interrupción de una instancia de spot, Amazon EC2 le notifica que la instancia de spot se interrumpirá en dos minutos y, transcurrido ese tiempo, se interrumpe la instancia.

El servicio subyacente que realiza la interrupción de la instancia de spot es AWS Fault Injection Service (AWS FIS). Para obtener más información sobre AWS FIS, consulte AWS Fault Injection Service.

> **Note**
>
> Los comportamientos de interrupción son `terminate`, `stop` y `hibernate`. Si establece el comportamiento de interrupción en `hibernate`, al iniciar una interrupción de una instancia de spot, el proceso de hibernación comenzará inmediatamente.

El inicio de una interrupción de una instancia de spot es compatible con todas las Regiones de AWS, excepto Asia-Pacífico (Yakarta), Asia-Pacífico (Osaka), China (Pekín) y China (Ningxia) y Oriente Medio (EAU).

Temas

- Inicio de una interrupción de instancias de spot
- Verificación de la interrupción de instancias de spot
- Cuotas

Inicio de una interrupción de instancias de spot

Puede utilizar la consola de EC2 para iniciar rápidamente una interrupción de una instancia de spot. Al seleccionar una solicitud de instancia de spot, puede iniciar la interrupción de una instancia de

spot. Al seleccionar una solicitud de flota de spot, puede iniciar la interrupción de varias instancias de spot a la vez.

Si desea realizar experimentos más avanzados para probar las interrupciones de instancias de spot, puede crear sus propios experimentos con la consola AWS FIS.

Para iniciar una interrupción de una instancia de spot en una solicitud de instancia de spot mediante la consola de EC2

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Spot Requests (Solicitudes de spot).
3. Seleccione una solicitud de instancia de spot y, a continuación, elija Actions (Acciones), Initiate interrumption (Iniciar interrupción). No puede seleccionar varias solicitudes de instancia de spot para iniciar una interrupción.
4. En el cuadro de diálogo Initiate Spot Instance interruption (Iniciar la interrupción de instancias de spot), en Service access (Acceso a los servicios), utilice el rol predeterminado o seleccione uno existente. Para elegir un rol existente, seleccione Usar un rol de servicio existente y, a continuación, en Rol de IAM, seleccione el rol que desea usar.
5. Cuando tenga todo listo para iniciar la interrupción de instancias de spot, seleccione Initiate interruption (Iniciar interrupción).

Para iniciar la interrupción de una o más instancias de spot en una solicitud de flota de spot mediante la consola de EC2

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Spot Requests (Solicitudes de spot).
3. Seleccione una solicitud de flota de spot y, a continuación, elija Acciones, Iniciar interrupción. No puede seleccionar varias solicitudes de flota de spot para iniciar una interrupción.
4. En el cuadro de diálogo Especifique el número de instancias de spot, en Número de instancias a interrumpir, introduzca el número de instancias de spot que se van a interrumpir y, a continuación, seleccione Confirmar.

> **Note**
>
> El número no puede superar el número de instancias de spot de la flota ni su cuota de instancias de spot que AWS FIS puede interrumpir por experimento.

5. En el cuadro de diálogo Initiate Spot Instance interruption (Iniciar la interrupción de instancias de spot), en Service access (Acceso a los servicios), utilice el rol predeterminado o seleccione uno existente. Para elegir un rol existente, seleccione Usar un rol de servicio existente y, a continuación, en Rol de IAM, seleccione el rol que desea usar.
6. Cuando tenga todo listo para iniciar la interrupción de instancias de spot, seleccione Initiate interruption (Iniciar interrupción).

Para crear experimentos más avanzados a fin de probar las interrupciones de instancias de spot con la consola AWS FIS

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Spot Requests.
3. Seleccione Actions (Acciones), Create advanced experiments (Creación de experimentos avanzados).

   Se abrirá la consola de AWS FIS. Para obtener más información, consulte Tutorial: pruebe las interrupciones de instancias de spot con AWS FIS en la Guía del usuario de AWS Fault Injection Service.

Verificación de la interrupción de instancias de spot

Después de iniciar la interrupción, ocurre lo siguiente:

- La instancia de spot recibe una recomendación de reequilibrio de instancias.
- Se emite un aviso de interrupción de instancia de spot dos minutos antes de que AWS FIS interrumpa la instancia.
- Cuando pasan dos minutos, la instancia de spot se interrumpe.
- Una instancia de spot que detuvo AWS FIS permanece detenida hasta que la reinicie.

Para comprobar que la instancia se interrumpió después de que iniciara la interrupción

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, abra Spot Requests (Solicitudes de spot) e Instances (instancia[s]) en pestañas o ventanas separadas del navegador.

3. En Solicitudes de spot, seleccione la solicitud de instancia de spot o la solicitud de flota de spot. El estado inicial es.`fulfilled` Una vez interrumpida la instancia, el estado cambia de la siguiente forma, según el comportamiento de la interrupción:
   - `terminate`: el estado cambia a `instance-terminated-by-experiment`.
   - `stop`: el estado cambia a `marked-for-stop-by-experiment` y, a continuación, a `instance-stopped-by-experiment`.
4. En Instances (instancia[s]), seleccione la instancia de spot. El estado inicial es.`Running` Dos minutos después de recibir el aviso de interrupción de la instancia de spot, el estado cambia de la siguiente forma, según el comportamiento de la interrupción:
   - `stop`: el estado cambia a `Stopping` y, a continuación, a `Stopped`.
   - `terminate`: el estado cambia a `Shutting-down` y, a continuación, a `Terminated`.

Cuotas

Su Cuenta de AWS tiene la siguiente cuota predeterminada para el número de instancias de spot que AWS FIS puede interrumpir por experimento.

Nombre	Valor predeterminado	Ajustable	Descripción
instancias de spot de destino para aws:ec2:send-spot-instance-interruptions	Cada región admitida: 5	Sí	El número máximo de instancias de spot a las que aws:ec2:send-spot-instance-interruptions puede dirigirse al identificar los objetivos mediante etiquetas, por experimento.

Puede solicitar un aumento de cuota. Para obtener más información, consulte Solicitud de un aumento de cuota en la Guía del usuario de Service Quotas.

Para ver todas las cuotas de AWS FIS, abra la consola de Service Quotas. En el panel de navegación, elija servicios de AWS y seleccione AWS Fault Injection Service. También, puede ver

todas las Cuotas para AWS Fault Injection Service en la Guía del usuario de AWS Fault Injection Service.

Avisos de interrupción de instancias de spot.

Un aviso de interrupción de instancia de spot es una advertencia que se emite dos minutos antes de que Amazon EC2 termine o detenga una instancia de spot. Si especifica la hibernación como comportamiento de interrupción, recibe un aviso de interrupción, pero no recibe una advertencia de dos minutos, ya que el proceso de hibernación comienza de inmediato.

La mejor manera de gestionar las interrupciones de instancias de spot correctamente es diseñar su aplicación para que sea tolerante a errores. Para lograrlo, puede aprovechar los avisos de interrupción de instancias de spot. Le recomendamos que compruebe estos avisos de interrupción cada 5 segundos.

Los avisos de interrupción están disponibles como CloudWatch Events y como elementos en los metadatos de instancia en la instancia de spot. Los avisos de interrupción se emiten en la medida de lo posible.

EC2 Spot Instance interruption notice

Cuando Amazon EC2 va a interrumpir su instancia de spot, emite un evento dos minutos antes de la interrupción real (excepto en los casos en los que hay hibernación, que recibe el aviso de interrupción, pero no con dos minutos de antelación porque la hibernación comienza de inmediato). Amazon EventBridge puede detectar este evento. Para obtener más información, consulte los Eventos de Amazon EventBridge en la Guía del usuario de Amazon EventBridge. Para obtener un ejemplo detallado que le explica cómo crear y utilizar reglas de eventos, consulte Aprovechamiento de los avisos de interrupción de instancias de spot de Amazon EC2.

El siguiente es un ejemplo de evento de interrupción de una instancia de spot. Los valores posibles de `instance-action` son `hibernate`, `stop`, o `terminate`.

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-123456789012",
    "detail-type": "EC2 Spot Instance Interruption Warning",
    "source": "aws.ec2",
    "account": "123456789012",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-2",
```

```
    "resources": ["arn:aws:ec2:us-east-2a:instance/i-1234567890abcdef0"],
    "detail": {
        "instance-id": "i-1234567890abcdef0",
        "instance-action": "action"
    }
}
```

> **Note**
>
> El formato del ARN del evento de interrupción de la instancia de spot es `arn:aws:ec2:availability-zone:instance/instance-id`. Este formato es distinto del formato del ARN del recurso de EC2.

instance-action

Si Amazon EC2 ha marcado una instancia de spot para detenerla o terminarla, el elemento `instance-action` está presente en los metadatos de la instancia. De lo contrario, no está presente. Puede recuperar la `instance-action` mediante el Servicio de metadatos de instancia, versión 2 (IMDSv2) de la siguiente manera.

Utilice el comando correspondiente a su sistema operativo.

Linux

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/spot/instance-action
```

Windows

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/meta-data/spot/instance-action
```

El elemento `instance-action` especifica la acción (parar o terminar) y la hora aproximada en UTC a la que se producirá.

En el siguiente ejemplo de salida, se indica la hora a la que se detendrá esta instancia.

```
{"action": "stop", "time": "2017-09-18T08:22:00Z"}
```

En el siguiente ejemplo de salida, se indica la hora a la que terminará esta instancia.

```
{"action": "terminate", "time": "2017-09-18T08:22:00Z"}
```

Si Amazon EC2 no está preparándose para detener o terminar la instancia o si terminó la instancia usted mismo, `instance-action` no está presente en los metadatos de la instancia y recibe un mensaje de error HTTP 404 cuando intenta recuperarlo.

termination-time

Este elemento se conserva para ofrecer compatibilidad con versiones anteriores. En su lugar, utilice `instance-action`.

Si Amazon EC2 marca su instancia de spot para la finalización (ya sea debido a una interrupción de la instancia de spot en la que el comportamiento de interrupción está establecido como `terminate` o debido a la cancelación de una solicitud de instancia de spot persistente), el elemento `termination-time` está presente en los metadatos de la instancia. De lo contrario, no está presente. Puede recuperar `termination-time` mediante el IMDSv2 de la siguiente manera.

Utilice el comando correspondiente a su sistema operativo.

Linux

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-
ec2-metadata-token-ttl-seconds: 21600"`
[ec2-user ~]$ if curl -H "X-aws-ec2-metadata-token: $TOKEN" -s http://169.254.169.254/
latest/meta-data/spot/termination-time | grep -q .*T.*Z; then echo
 termination_scheduled; fi
```

Windows

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/meta-data/spot/
termination-time
```

El elemento `termination-time` especifica la hora aproximada, en UTC, a la que la instancia recibirá la señal de cierre. A continuación, se muestra un ejemplo del resultado.

```
2015-01-05T18:02:00Z
```

Si Amazon EC2 no está preparándose para finalizar la instancia (ya sea porque no hay ninguna interrupción de la instancia de spot o porque el comportamiento de interrupción está establecido como `stop` o `hibernate`) o si finalizó la instancia de spot usted mismo, el elemento `termination-time` no está presente en los metadatos de la instancia (por lo que recibe un mensaje de error HTTP 404) o contiene un valor que no es un valor de hora.

Si Amazon EC2 no es capaz de terminar la instancia, el estado de la solicitud se establece en `fulfilled`. El valor `termination-time` permanece en los metadatos de la instancia con la hora aproximada original, que ahora ya está en el pasado.

Buscar instancias de spot interrumpida

En la consola, el panel Instances (instancia[s]) muestra todas las instancias, incluida instancias de spot. El ciclo de vida de instancia de una instancia de spot es `spot`. El estado de instancia de una instancia de spot es `stopped` o `terminated`, según el comportamiento de interrupción que haya configurado. Para una instancia de spot en estado de hibernación, el estado de la instancia es `stopped`.

Para encontrar una instancia de spot interrumpida mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Aplicque el siguiente filtro: Instance lifecycle=spot.
4. Aplique los filtros Instance state=stopped o Instance state=terminated en función del comportamiento de interrupción que haya configurado.
5. Para cada instancia de spot, en la pestaña Detalles, dentro de Detalles de la instancia, busque Mensaje de transición de estado. Los siguientes códigos indican que la instancia de spot se interrumpió.
   - `Server.SpotInstanceShutdown`
   - `Server.SpotInstanceTermination`
6. Para obtener más información sobre el motivo de la interrupción, compruebe el código de estado de la solicitud de spot. Para obtener más información, consulte the section called “Estado de las solicitudes de spot”.

Buscar instancias de spot interrumpidas mediante la AWS CLI

Puede enumerar las interrupciones de instancias de spot mediante el comando describe-instances con el parámetro `--filters`. Para enumerar solo los ID de instancias en la salida, incluya el parámetro `--query`.

Si el comportamiento de interrupción de instancias es terminar las instancias de spot, utilice el siguiente comando:

```
aws ec2 describe-instances \
    --filters Name=instance-lifecycle,Values=spot Name=instance-state-
name,Values=terminated Name=state-reason-code,Values=Server.SpotInstanceTermination \
    --query "Reservations[*].Instances[*].InstanceId"
```

Si el comportamiento de interrupción de instancias es detener las instancias de spot, utilice el siguiente comando:

```
aws ec2 describe-instances \
    --filters Name=instance-lifecycle,Values=spot Name=instance-state-
name,Values=stopped Name=state-reason-code,Values=Server.SpotInstanceShutdown \
    --query "Reservations[*].Instances[*].InstanceId"
```

Cómo determinar si Amazon EC2 interrumpió una instancia de spot

Si se detiene una instancia de spot, puede utilizar CloudTrail para ver si Amazon EC2 interrumpió la instancia de spot. En AWS CloudTrail, el nombre del evento `BidEvictedEvent` indica que Amazon EC2 interrumpió la instancia de spot.

Para ver eventos BideVicteDevent en CloudTrail

1. Abra la consola de CloudTrail en https://console.aws.amazon.com/cloudtrail/.
2. En el panel de navegación, elija Event history (Historial de eventos).
3. En el menú desplegable de filtros, elija Nombre del evento y, a continuación, en el campo de filtro de la derecha, escriba BideVicteDevent.
4. Seleccionar BideVicteDevent en la lista resultante para ver sus detalles. En Event record (Registro de evento), puede encontrar el ID de instancia.

Para obtener más información acerca del uso de CloudTrail, consulte Registro de llamadas a la API de Amazon EC2 mediante AWS CloudTrail.

Facturación de las instancias de spot interrumpidas

Cuando una instancia de spot se ve interrumpida, se aplican los cargos de instancia y volumen de EBS, junto con otros posibles cargos, de la siguiente forma.

Uso de instancias

Quién interrumpe la instancia de spot	Sistema operativo	Interrumpida en la primera hora	Interrumpida cualquier hora después de la primera hora
Si usted detiene o termina la instancia de spot	Windows y Linux (excepto SUSE)	Se cobra por los segundos utilizados	Se cobra por los segundos utilizados
	SUSE	Se cobra la hora completa aunque no se utilice durante toda la hora	Se cobran las horas completas de uso y se cobra una hora completa para la hora parcial en la que se produjo la interrupción
Si Amazon EC2 interrumpe la instancia de spot	Windows y Linux (excepto SUSE)	No se aplican cargos	Se cobra por los segundos utilizados
	SUSE	No se aplican cargos	Se cobran las horas completas de uso, pero no se cobra la hora parcial en la que se produjo la interrupción

Uso de volúmenes de EBS

Mientras una instancia de spot interrumpida está detenida, solo se le cobran los volúmenes de EBS, los cuales se conservan.

Con la flota de EC2 y la flota de spot, si tiene muchas instancias detenidas, puede superar el límite de la cantidad de volúmenes de EBS de su cuenta.

Otros cargos

Si su instancia de spot en ejecución incurre en cargos por otros servicios, como la transferencia de datos, las direcciones IP elásticas o el uso de otros servicios administrados por AWS, se le facturará por su uso. Esto es independiente de quién interrumpa la instancia de spot o cuándo se interrumpió. Incluso si no se le cobra por el uso de la instancia de spot cuando Amazon EC2 interrumpe su instancia de spot en la primera hora, puede incurrir en otros cargos.

Para obtener más información, consulte Precios de Amazon EC2 bajo demanda.

Puntuación de ubicación de spot

La característica de puntuación de ubicación de spot puede recomendar una región o zona de disponibilidad de AWS según sus requisitos de capacidad de spot. La capacidad de spot fluctúa y no se puede estar seguro de que siempre se obtendrá la capacidad necesaria. La puntuación de ubicación de spot indica la probabilidad de que una solicitud de spot tenga éxito en una región o zona de disponibilidad.

> **Note**
>
> La puntuación de ubicación de spot no proporciona ninguna garantía en términos de capacidad disponible o riesgo de interrupción. Una puntuación de ubicación de spot solo sirve como recomendación.

Beneficios

Puede utilizar la característica de puntuación de ubicación de spot para lo siguiente:

- Reubicar y escalar la capacidad de computación de spot en una región diferente, según sea necesario, en respuesta al aumento de las necesidades de capacidad o a la disminución de la capacidad disponible en la región actual.
- Identificar la zona de disponibilidad más óptima en la que ejecutar cargas de trabajo de zona de disponibilidad única.
- Para simular las futuras necesidades de capacidad de spot para que pueda elegir una región óptima para la expansión de las cargas de trabajo basadas en spot.
- Para encontrar una combinación óptima de tipos de instancias que satisfagan sus necesidades de capacidad de spot.

Temas

Costes

No se aplican cargos adicionales por el uso de la característica de puntuación de ubicación de spot.

Cómo funciona la puntuación de ubicación de spot

Cuando se utiliza la característica de puntuación de ubicación de spot, primero se deben especificar los requisitos de computación para las instancias de spot, y luego Amazon EC2 devuelve las 10 mejores regiones o las zonas de disponibilidad donde es probable que la solicitud de spot tenga éxito. Cada región o zona de disponibilidad se califica en una escala del 1 al 10: 10 indica que es muy probable que la solicitud de spot tenga éxito y 1 indica que no es probable que la solicitud de spot tenga éxito.

Para utilizar la característica de puntuación de ubicación de spot, siga estos pasos:

- Paso 1: especificar los requisitos de spot
- Paso 2: filtrar la respuesta de puntuación de ubicación de spot
- Paso 3: revisar las recomendaciones
- Paso 4: utilizar las recomendaciones

Paso 1: especificar los requisitos de spot

En primer lugar, especifique la capacidad de spot de destino deseada y los requisitos de computación, de la siguiente manera:

1. Especifique la capacidad de spot de destino y, opcionalmente, la unidad de capacidad de destino.

   Puede especificar la capacidad de spot de destino deseada en términos del número de instancias o vCPU, o en términos de la cantidad de memoria en MiB. Para especificar la capacidad de destino en número de vCPU o cantidad de memoria, debe especificar la unidad de capacidad de destino como `vcpu` o `memory-mib`. De lo contrario, el valor predeterminado es el número de instancias.

   Al especificar la capacidad de destino en función del número de vCPU o la cantidad de memoria, puede utilizar estas unidades al contar la capacidad total. Por ejemplo, si desea utilizar una combinación de instancias de distintos tamaños, puede especificar la capacidad de destino como un número total de vCPU. A continuación, la característica de puntuación de ubicación de spot considera cada tipo de instancia de la solicitud por su número de vCPU y cuenta el número total de vCPU en lugar del número total de instancias al sumar la capacidad de destino total.

Por ejemplo, supongamos que especifica una capacidad de destino total de 30 vCPU y la lista de tipos de instancia consta de c5.xlarge (4 vCPU), m5.2xlarge (8 vCPU) y r5.large (2 vCPU). Para lograr un total de 30 vCPU, podría obtener una combinación de 2 c5.xlarge (2*4 vCPU), 2 m5.2xlarge (2*8 vCPU) y 3 r5.large (3*2 vCPU).

2. Especifique tipos de instancia o atributos de instancia.

   Puede especificar los tipos de instancia que se van a utilizar o bien especificar los atributos de instancia que necesita para los requerimientos de computación y, a continuación, permitir que Amazon EC2 identifique los tipos de instancia que tienen esos atributos. Esto se conoce como selección de tipo de instancia basada en atributos.

   No se pueden especificar los tipos de instancia y los atributos de instancia en la misma solicitud de puntuación de ubicación de spot.

   Si especifica tipos de instancias, debe especificar al menos tres tipos de instancia diferentes; de lo contrario, Amazon EC2 devolverá una puntuación de ubicación de spot baja. Del mismo modo, si especifica atributos de instancia, deben resolverse en al menos tres tipos de instancias diferentes.

Para ver ejemplos de diferentes formas de especificar los requisitos de spot, consulte Configuraciones de ejemplo.

Paso 2: filtrar la respuesta de puntuación de ubicación de spot

Amazon EC2 calcula la puntuación de ubicación de spot de cada región o zona de disponibilidad y devuelve las 10 mejores regiones o las 10 mejores zonas de disponibilidad en las que es más probable que su solicitud de spot tenga éxito. De forma predeterminada, se devuelve una lista de regiones puntuadas. Si planea iniciar toda la capacidad de spot en una única zona de disponibilidad, resulta útil solicitar una lista de zonas de disponibilidad puntuadas.

Puede especificar un filtro de región para restringir las regiones que se devolverán en la respuesta.

Puede combinar el filtro de región y una solicitud de zonas de disponibilidad puntuadas. De este modo, las zonas de disponibilidad puntuadas se limitan a las regiones para las que ha filtrado. Para encontrar la zona de disponibilidad con mayor puntuación de una región, especifique solo esa región y la respuesta devolverá una lista puntuada de todas las zonas de disponibilidad de esa región.

Paso 3: revisar las recomendaciones

La puntuación de ubicación de spot para cada región o zona de disponibilidad se calcula en función de la capacidad de destino, la composición de los tipos de instancia, las tendencias de uso de spot históricas y actuales y la hora de la solicitud. Debido a que la capacidad de spot fluctúa constantemente, la misma solicitud de puntuación de ubicación de spot puede producir puntuaciones diferentes cuando se calcula en diferentes momentos.

Las regiones y las zonas de disponibilidad se califican en una escala del 1 al 10. Una puntuación de 10 indica que es altamente probable (aunque no está garantizado) que la solicitud de spot tenga éxito. Una puntuación de 1 indica que no es probable que la solicitud de spot tenga éxito. Es posible que se devuelva la misma puntuación para distintas regiones o zonas de disponibilidad.

Si se devuelven puntuaciones bajas, puede editar los requisitos de computación y volver a calcular la puntuación. También puede solicitar recomendaciones de puntuación de ubicación de spot para los mismos requisitos de computación en diferentes momentos del día.

Paso 4: utilizar las recomendaciones

Una puntuación de ubicación de spot solo es relevante si la solicitud de spot tiene exactamente la misma configuración que la configuración de puntuación de ubicación de spot (capacidad de destino, unidad de capacidad de destino y tipos de instancias o atributos de instancia) y está configurada para utilizar la estrategia de asignación `capacity-optimized`. De lo contrario, la probabilidad de obtener capacidad de spot disponible no estará alineada con la puntuación.

Si bien una puntuación de ubicación de spot sirve de guía y ninguna puntuación garantiza que su solicitud de spot se cumpla total o parcialmente, puede utilizar la siguiente información para obtener mejores resultados:

- Utilice la misma configuración: la puntuación de ubicación de spot solo es relevante si la configuración de la solicitud de spot (capacidad de destino, unidad de capacidad de destino y tipos de instancia o atributos de instancia) del grupo de escalado automático, flota de EC2 o flota de spot es la misma que la especificada para obtener la puntuación de ubicación de spot.

  Si ha utilizado la selección de tipo de instancia basada en atributos en la solicitud de puntuación de ubicación de spot, puede utilizar la selección de tipo de instancia basada en atributos para configurar el grupo de escalado automático, la flota de EC2 o la flota de spot. Para obtener más información, consulte Creación de un grupo de Auto Scaling con un conjunto de requisitos en los tipos de instancia utilizados, Selección de tipo de instancia basada en atributos para la flota de EC2 y Selección de tipo de instancia basada en atributos para la flota de spot.

> **Note**
>
> Si especificó la capacidad de destino en términos del número de vCPU o la cantidad de memoria y ha especificado tipos de instancias en la configuración de puntuación de ubicación de spot, tenga en cuenta que no puede crear esta configuración en el grupo de escalado automático, la flota de EC2 o la flota de spot. En su lugar, debe configurar de forma manual la ponderación de la instancia mediante el parámetro `WeightedCapacity`.

- Utilice la estrategia de asignación **`capacity-optimized`**: todas las puntuaciones presuponen que, para que la solicitud de capacidad de spot tenga éxito, la solicitud de flota se configurará de modo que utilice todas las zonas de disponibilidad (para solicitar capacidad en la totalidad de regiones) o una única zona de disponibilidad (si se solicita capacidad en una sola zona de disponibilidad) y la estrategia de asignación de spot `capacity-optimized`. Si utiliza otras estrategias de asignación, como `lowest-price`, la probabilidad de obtener capacidad de spot disponible no estará alineada con la puntuación.
- Actúe según indique la puntuación de forma inmediata: la recomendación de puntuación de ubicación de spot refleja la capacidad de spot disponible en el momento de la solicitud, y la misma configuración puede producir puntuaciones diferentes cuando se calcula en diferentes momentos debido a las fluctuaciones de la capacidad de spot. Si bien una puntuación de 10 significa que es muy probable que su solicitud de capacidad de spot tenga éxito (aunque esto no esté garantizado) para obtener los mejores resultados le recomendamos que actúe con relación a la puntuación en forma inmediata. También le recomendamos que obtenga una nueva puntuación cada vez que intente una solicitud de capacidad.

Limitaciones

- Límite de capacidad de destino: el límite de capacidad de destino de la puntuación de ubicación de spot se basa en el uso reciente de spot, a la vez que tiene en cuenta el posible crecimiento en el uso. Si no ha habido un uso reciente de spot, se proporciona un límite predeterminado bajo alineado con el límite de solicitudes de spot.
- Límite de configuraciones de solicitudes: se puede limitar el número de nuevas configuraciones de solicitudes en un periodo de 24 horas si se detectan patrones no asociados con el uso previsto de la característica de puntuación de ubicación de spot. Si se alcanza el límite, se puede volver a intentar con las configuraciones de solicitud que ya han sido utilizadas, pero no se puede especificar nuevas configuraciones de solicitud hasta el próximo periodo de 24 horas.

- Número mínimo de tipos de instancias: si especifica tipos de instancias, debe especificar al menos tres tipos de instancias diferentes; de lo contrario, Amazon EC2 devolverá una puntuación de ubicación de spot baja. Del mismo modo, si especifica atributos de instancia, deben resolverse en al menos tres tipos de instancias diferentes. Los tipos de instancias se consideran diferentes si tienen un nombre distinto. Por ejemplo, m5.8xlarge, m5a.8xlarge y m5.12xlarge se consideran diferentes.

Permiso de IAM necesarios

De forma predeterminada, las identidades de IAM (usuarios, roles o grupos) no tienen permiso para utilizar la característica de puntuación de ubicación de spot. Para permitir que las identidades de IAM utilicen la característica de puntuación de ubicación de spot, debe crear una política de IAM que conceda permiso para utilizar la acción de la API de EC2 `ec2:GetSpotPlacementScores`. A continuación, adjunte la política a la identidad de IAM que requiere el permiso.

A continuación, se muestra un ejemplo de política de IAM que concede permisos para la acción de la API de EC2 `ec2:GetSpotPlacementScores`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:GetSpotPlacementScores",
            "Resource": "*"
        }
    ]
}
```

Para obtener más información acerca de la actualización de políticas de IAM, consulte Edición de políticas de IAM en la Guía del usuario de IAM.

Para dar acceso, agregue permisos a los usuarios, grupos o roles:

- Usuarios y grupos en AWS IAM Identity Center:

  Cree un conjunto de permisos. Siga las instrucciones de Creación de un conjunto de permisos en la Guía del usuario de AWS IAM Identity Center.
- Usuarios administrados en IAM a través de un proveedor de identidades:

Cree un rol para la federación de identidades. Siga las instrucciones descritas en Creación de un rol para un proveedor de identidad de terceros (federación) en la Guía del usuario de IAM.

- Usuarios de IAM:
  - Cree un rol que el usuario pueda aceptar. Siga las instrucciones descritas en Creación de un rol para un usuario de IAM en la Guía del usuario de IAM.
  - (No recomendado) Adjunte una política directamente a un usuario o añada un usuario a un grupo de usuarios. Siga las instrucciones descritas en Adición de permisos a un usuario (consola) de la Guía del usuario de IAM.

Calcular una puntuación de ubicación de spot

Puede calcular una puntuación de ubicación de spot mediante la consola de Amazon EC2 o la AWS CLI.

Temas

- Calcular una puntuación de ubicación de spot mediante la especificación de atributos de instancia (consola)
- Calcular una puntuación de ubicación de spot mediante la especificación de tipos de instancias (consola)
- Calcular una puntuación de ubicación de spot (AWS CLI)

Calcular una puntuación de ubicación de spot mediante la especificación de atributos de instancia (consola)

Para calcular una puntuación de ubicación de spot mediante la especificación de atributos de instancia

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Solicitudes de spot.
3. Elija Spot placement score (Puntuación de ubicación de spot).
4. Elija Enter requirements (Ingresar requisitos).
5. En Target capacity (Capacidad de destino), ingrese la capacidad deseada en función del número de instancias o vCPU, o la cantidad de memoria (MiB).

6. Para los Requisitos de tipo de instancia, a fin de especificar sus requisitos de computación y permitir que Amazon EC2 identifique los tipos de instancias óptimos en relación con estos requisitos, elija Especificar los atributos de instancia que coincidan con los requisitos de computación.
7. En vCPU, ingrese el número mínimo y máximo deseado de vCPU. Para no especificar ningún límite, seleccione No minimum (Sin mínimo), No maximum (Sin máximo) o ambos.
8. En Memory (GiB) (Memoria [GiB]), ingrese la cantidad mínima y máxima de memoria deseada. Para no especificar ningún límite, seleccione No minimum (Sin mínimo), No maximum (Sin máximo) o ambos.
9. En CPU architecture (Arquitectura de CPU), seleccione la arquitectura de instancias requerida.
10. (Opcional) En Additional instance attributes (Atributos de instancia adicionales), puede especificar opcionalmente uno o varios atributos para expresar sus requisitos de computación con más detalle. Cada atributo adicional agrega una restricción más a su solicitud. Puede omitir los atributos adicionales; si se omiten, se utilizan los valores predeterminados. Para obtener una descripción de cada atributo y de sus valores predeterminados, consulte get-spot-placement-scores en la Referencia de la línea de comandos de Amazon EC2.
11. (Opcional) Para ver los tipos de instancia con los atributos especificados, expanda Preview matching instance types (Vista previa de los tipos de instancia que coinciden). Para excluir que los tipos de instancias se utilicen en la evaluación de ubicación, seleccione las instancias y, a continuación, elija Exclude selected instance types (Excluir los tipos de instancias seleccionados).
12. Elija Load placement scores (Cargar puntuaciones de ubicación) y revise los resultados.
13. (Opcional) Para mostrar la puntuación de ubicación de spot para regiones específicas, en Regiones que se deben evaluar, seleccione las regiones que desea evaluar y, a continuación, elija Calcular las puntuaciones de ubicación.
14. (Opcional) Para mostrar la puntuación de ubicación de spot de las zonas de disponibilidad de las regiones mostradas, seleccione la casilla de verificación Provide placement scores per Availability Zone (Proporcionar puntuaciones de ubicación por zona de disponibilidad). Le resultará útil contar con una lista de zonas de disponibilidad puntuadas cuando quiera iniciar toda la capacidad de spot en una única zona de disponibilidad.
15. (Opcional) Para editar los requisitos de computación y obtener una nueva puntuación de ubicación, elija Edit (Editar), realice los ajustes necesarios y, a continuación, elija Calculate placement scores (Calcular la puntuación de ubicación).

Calcular una puntuación de ubicación de spot mediante la especificación de tipos de instancias (consola)

Para calcular una puntuación de ubicación de spot mediante la especificación de tipos de instancias

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Solicitudes de spot.
3. Elija Spot placement score (Puntuación de ubicación de spot).
4. Elija Enter requirements (Ingresar requisitos).
5. En Target capacity (Capacidad de destino), ingrese la capacidad deseada en función del número de instancias o vCPU, o la cantidad de memoria (MiB).
6. Para Instance type requirements (Requisitos del tipo de instancia), para especificar los tipos de instancia que desea utilizar, elija Manually select instance types (Seleccionar manualmente los tipos de instancia).
7. Elija Select instance types (Seleccionar tipos de instancia), seleccione los tipos de instancia que desea utilizar y, a continuación, elija Select (Seleccionar). Para buscar rápidamente tipos de instancias, puede utilizar la barra de filtros y así filtrar los tipos de instancia por diferentes propiedades.
8. Elija Load placement scores (Cargar puntuaciones de ubicación) y revise los resultados.
9. (Opcional) Para mostrar la puntuación de ubicación de spot para regiones específicas, en Regiones que se deben evaluar, seleccione las regiones que desea evaluar y, a continuación, elija Calcular las puntuaciones de ubicación.
10. (Opcional) Para mostrar la puntuación de ubicación de spot de las zonas de disponibilidad de las regiones mostradas, seleccione la casilla de verificación Provide placement scores per Availability Zone (Proporcionar puntuaciones de ubicación por zona de disponibilidad). Le resultará útil contar con una lista de zonas de disponibilidad puntuadas cuando quiera iniciar toda la capacidad de spot en una única zona de disponibilidad.
11. (Opcional) Para editar la lista de tipos de instancia y obtener una nueva puntuación de ubicación, elija Edit (Editar), realice los ajustes necesarios y, a continuación, elija Calculate placement scores (Calcular puntuaciones de ubicación).

Calcular una puntuación de ubicación de spot (AWS CLI)

Para calcular la puntuación de ubicación de spot

1. (Opcional) Para generar todos los parámetros posibles que se pueden especificar para la configuración de puntuación de ubicación de spot, utilice el comando get-spot-placement-scores y el parámetro `--generate-cli-skeleton`.

```
aws ec2 get-spot-placement-scores \
    --region us-east-1 \
    --generate-cli-skeleton
```

Resultado previsto

```
{
    "InstanceTypes": [
        ""
    ],
    "TargetCapacity": 0,
    "TargetCapacityUnitType": "vcpu",
    "SingleAvailabilityZone": true,
    "RegionNames": [
        ""
    ],
    "InstanceRequirementsWithMetadata": {
        "ArchitectureTypes": [
            "x86_64_mac"
        ],
        "VirtualizationTypes": [
            "hvm"
        ],
        "InstanceRequirements": {
            "VCpuCount": {
                "Min": 0,
                "Max": 0
            },
            "MemoryMiB": {
                "Min": 0,
                "Max": 0
            },
            "CpuManufacturers": [
                "amd"
```

```
            ],
            "MemoryGiBPerVCpu": {
                "Min": 0.0,
                "Max": 0.0
            },
            "ExcludedInstanceTypes": [
                ""
            ],
            "InstanceGenerations": [
                "previous"
            ],
            "SpotMaxPricePercentageOverLowestPrice": 0,
            "OnDemandMaxPricePercentageOverLowestPrice": 0,
            "BareMetal": "excluded",
            "BurstablePerformance": "excluded",
            "RequireHibernateSupport": true,
            "NetworkInterfaceCount": {
                "Min": 0,
                "Max": 0
            },
            "LocalStorage": "included",
            "LocalStorageTypes": [
                "hdd"
            ],
            "TotalLocalStorageGB": {
                "Min": 0.0,
                "Max": 0.0
            },
            "BaselineEbsBandwidthMbps": {
                "Min": 0,
                "Max": 0
            },
            "AcceleratorTypes": [
                "fpga"
            ],
            "AcceleratorCount": {
                "Min": 0,
                "Max": 0
            },
            "AcceleratorManufacturers": [
                "amd"
            ],
            "AcceleratorNames": [
                "vu9p"
```

```
            ],
            "AcceleratorTotalMemoryMiB": {
                "Min": 0,
                "Max": 0
            }
        }
    },
    "DryRun": true,
    "MaxResults": 0,
    "NextToken": ""
}
```

2. Cree un archivo de configuración JSON con el resultado del paso anterior y configúrelo de la siguiente manera:

   a. En `TargetCapacity` (Capacidad de destino), ingrese la capacidad de spot deseada en función del número de instancias o vCPU, o la cantidad de memoria (MiB).

   b. En `TargetCapacityUnitType`, ingrese la unidad correspondiente a la capacidad de destino. Si omite este parámetro, el valor predeterminado será `units`.

      Valores válidos: `units` (lo que se traduce en número de instancias) |`vcpu` | `memory-mib`

   c. En `SingleAvailabilityZone`, especifique `true` para una respuesta que devuelva una lista de zonas de disponibilidad puntuadas. Le resultará útil contar con una lista de zonas de disponibilidad puntuadas cuando quiera iniciar toda la capacidad de spot en una única zona de disponibilidad. Si omite este parámetro, se establece de manera predeterminada como `false` y la respuesta devuelve una lista de regiones puntuadas.

   d. (Opcional) En `RegionNames`, especifique las regiones que desea utilizar como filtro. Debe especificar el código de la región; por ejemplo, `us-east-1`.

      Con un filtro de región, la respuesta devuelve solo las regiones que especifique. Si ha especificado `true` para `SingleAvailabilityZone`, la respuesta devuelve solo las zonas de disponibilidad de las regiones que haya especificado.

   e. Puede incluir bien `InstanceTypes` o bien `InstanceRequirements`, pero no se pueden usar ambos en la misma configuración.

      Especifique una de las siguientes opciones en la configuración JSON:

      - Para especificar una lista de los tipos de instancia, especifique los tipos de instancia en el parámetro `InstanceTypes`. Especifique al menos tres tipos de instancia diferentes. Si

especifica solo uno o dos tipos de instancia, la puntuación de ubicación de spot devuelve una puntuación baja. Para obtener la lista de los tipos de instancia, consulte Tipos de instancia de Amazon EC2.

- Para especificar los atributos de instancia de modo que Amazon EC2 identifique los tipos de instancia que coinciden con esos atributos, especifique los atributos que se encuentran en la estructura `InstanceRequirements`.

  Debe proporcionar valores para `VCpuCount`, `MemoryMiB` y `CpuManufacturers`. Puede omitir los demás atributos; cuando se omiten, se utilizan los valores predeterminados. Para obtener una descripción de cada atributo y de sus valores predeterminados, consulte get-spot-placement-scores en la Referencia de la línea de comandos de Amazon EC2.

Para ver configuraciones de ejemplo, consulte Configuraciones de ejemplo.

3. Para obtener la puntuación de ubicación de spot en relación con los requisitos especificados en el archivo JSON, utilice el comando get-spot-placement-scores y especifique el nombre y la ruta de acceso al archivo JSON mediante el parámetro `--cli-input-json`.

```
aws ec2 get-spot-placement-scores \
    --region us-east-1 \
    --cli-input-json file://file_name.json
```

Ejemplo de salida si `SingleAvailabilityZone` se establece como `false` o se omite (si se omite, se establece de manera predeterminada como `false`): se devuelve una lista de regiones puntuadas.

```
"SpotPlacementScores": [
    {
        "Region": "us-east-1",
        "Score": 7
    },
    {
        "Region": "us-west-1",
        "Score": 5
    },
   ...
```

Ejemplo de salida si `SingleAvailabilityZone` se establece en `true`; se devuelve una lista puntuada de zonas de disponibilidad.

```
"SpotPlacementScores": [
    {
        "Region": "us-east-1",
        "AvailabilityZoneId": "use1-az1"
        "Score": 8
    },
    {
        "Region": "us-east-1",
        "AvailabilityZoneId": "usw2-az3"
        "Score": 6
    },
   ...
```

Configuraciones de ejemplo

Cuando se utiliza la AWS CLI, se pueden utilizar las siguientes configuraciones de ejemplo.

Configuraciones de ejemplo

- Ejemplo: especificación de tipos de instancia y capacidad de destino
- Ejemplo: especificación de tipos de instancia y capacidad de destino en términos de memoria
- Ejemplo: especificar atributos para la selección de tipos de instancia basada en atributos
- Ejemplo: especificar atributos para la selección de tipos de instancia basada en atributos y devolver una lista puntuada de zonas de disponibilidad

Ejemplo: especificación de tipos de instancia y capacidad de destino

En la siguiente configuración de ejemplo, se especifican tres tipos de instancia diferentes y una capacidad de spot de 500 instancias de spot de destino.

```
{
    "InstanceTypes": [
        "m5.4xlarge",
        "r5.2xlarge",
        "m4.4xlarge"
    ],
```

```
    "TargetCapacity": 500
}
```

Ejemplo: especificación de tipos de instancia y capacidad de destino en términos de memoria

En la siguiente configuración de ejemplo se especifican tres tipos de instancia diferentes y una capacidad de spot de destino de 500 000 MiB de memoria, donde el número de instancias de spot que se van a iniciar debe proporcionar un total de 500 000 MiB de memoria.

```
{
    "InstanceTypes": [
        "m5.4xlarge",
        "r5.2xlarge",
        "m4.4xlarge"
    ],
    "TargetCapacity": 500000,
    "TargetCapacityUnitType": "memory-mib"
}
```

Ejemplo: especificar atributos para la selección de tipos de instancia basada en atributos

La siguiente configuración de ejemplo se configura para la selección de tipos de instancia basada en atributos y va seguida de una explicación de texto de la configuración de ejemplo.

```
{
    "TargetCapacity": 5000,
    "TargetCapacityUnitType": "vcpu",
    "InstanceRequirementsWithMetadata": {
        "ArchitectureTypes": ["arm64"],
        "VirtualizationTypes": ["hvm"],
        "InstanceRequirements": {
            "VCpuCount": {
                "Min": 1,
                "Max": 12
            },
            "MemoryMiB": {
                "Min": 512
            }
        }
    }
}
```

`InstanceRequirementsWithMetadata`

Para utilizar la selección de tipo de instancia basada en atributos, debe incluir la estructura `InstanceRequirementsWithMetadata` en la configuración y especificar los atributos deseados para las instancias de spot.

En el ejemplo anterior, se especifican los siguientes atributos de instancia requeridos:

- `ArchitectureTypes`: el tipo de arquitectura de los tipos de instancia debe ser `arm64`.
- `VirtualizationTypes`: el tipo de virtualización de los tipos de instancia debe ser `hvm`.
- `VCpuCount`: los tipos de instancia deben tener un mínimo de 1 y un máximo de 12 vCPU.
- `MemoryMiB`: los tipos de instancia deben tener un mínimo de 512 MiB de memoria. Al omitir el parámetro `Max`, indica que no hay límite máximo.

Tenga en cuenta que hay otros atributos opcionales que puede especificar. Para obtener una lista de atributos, consulte get-spot-placement-scores en la Referencia de la línea de comandos de Amazon EC2.

`TargetCapacityUnitType`

El parámetro `TargetCapacityUnitType` especifica la unidad de la capacidad de destino. En el ejemplo, la capacidad de destino es `5000` y el tipo de unidad de capacidad de destino es `vcpu`, que en conjunto especifican una capacidad de destino deseada de 5000 vCPU, en las que el número de instancias de spot que se van a iniciar debe proporcionar un total de 5000 vCPU.

Ejemplo: especificar atributos para la selección de tipos de instancia basada en atributos y devolver una lista puntuada de zonas de disponibilidad

El siguiente ejemplo de configuración, se configura para la selección de tipos de instancia basada en atributos. Al especificar `"SingleAvailabilityZone": true`, la respuesta devolverá una lista de zonas de disponibilidad puntuadas.

```
{
    "TargetCapacity": 1000,
    "TargetCapacityUnitType": "vcpu",
    "SingleAvailabilityZone": true,
    "InstanceRequirementsWithMetadata": {
        "ArchitectureTypes": ["arm64"],
        "VirtualizationTypes": ["hvm"],
        "InstanceRequirements": {
```

```
            "VCpuCount": {
                "Min": 1,
                "Max": 12
            },
            "MemoryMiB": {
                "Min": 512
            }
        }
    }
}
```

Fuente de datos de instancias de spot

Para ayudarlo a comprender los cargos de las instancias de spot, Amazon EC2 proporciona una fuente de datos que describe el uso que usted hace de las instancias de spot y los precios de estas. Esta fuente de datos se envía a un bucket de Amazon S3 que usted especifica al suscribirse a la fuente de datos.

Los archivos de fuente de datos llegan generalmente al bucket una vez cada hora, y cada hora de uso está registrada normalmente en un único archivo de datos. Estos archivos se comprimen (gzip) antes de que se entreguen al bucket. Amazon EC2 puede escribir varios archivos para una determinada hora de uso en la que los archivos sean grandes (por ejemplo, cuando el contenido del archivo para la hora exceda los 50 MB antes de comprimirlo).

> **Note**
>
> Solo puede crear una fuente de datos de instancias de spot por Cuenta de AWS. Si no tiene una instancia de spot en ejecución durante una determinada hora, no recibirá ningún archivo de fuente de datos para esa hora.

La fuente de datos de instancias de spot se admite en todas las regiones de AWS, excepto en China (Pekín), China (Ningxia), AWS GovCloud (EE. UU) y las Regiones desactivadas de forma predeterminada.

Contenido

- Describir la fuente de datos de instancias de spot
- Consulta de los datos de su fuente de datos
- Eliminar la fuente de datos de instancia de spot

Nombre y formato del archivo de fuente de datos

El nombre del archivo de fuente de datos de la instancia de spot usa el siguiente formato (con la fecha y la hora en UTC):

```
bucket-name.s3.amazonaws.com/optional-prefix/aws-account-id.YYYY-MM-DD-HH.n.unique-id.gz
```

Por ejemplo, si el nombre del bucket es **my-bucket-name** y el prefijo es **my-prefix**, los nombres de los archivos serán similares al siguiente ejemplo:

```
my-bucket-name.s3.amazonaws.com/my-prefix/111122223333.2023-12-09-07.001.b959dbc6.gz
```

Para obtener más información acerca de los nombres de bucket, consulte Reglas para la nomenclatura de bucket en la Guía del usuario de Amazon S3.

Los archivos de fuente de datos de instancia de spot están delimitados por tabuladores. Cada línea en el archivo de datos corresponde a una hora de instancia y contiene los campos enumerados en la siguiente tabla.

Campo	Descripción
`Timestamp`	La marca de tiempo que se usa para determinar el precio que se cobra por esta hora de instancia.
`UsageType`	El tipo de uso y el tipo de instancia por los que se le cobra. Para `m1.small` instancias de spot, este campo está establecido en `SpotUsage` . Para todos los demás tipos de instancias, este campo está establecido en `SpotUsage :` {instance-type}. Por ejemplo, `SpotUsage:c1.medium` .
`Operation`	

Campo	Descripción
	El producto por el que se le cobra. Para las instancias de spot de Linux, este campo está establecido en `RunInstances` . Para las instancias de spot de Windows, este campo está establecido en `RunInstances:0002` . El uso de spots se agrupa por zona de disponibilidad.
`InstanceID`	El ID de la instancia de spot que generó este uso de instancia.
`MyBidID`	El ID de la solicitud de instancia de spot que generó este uso de instancia.
`MyMaxPrice`	El precio máximo especificado para esta solicitud de spot.
`MarketPrice`	El precio de spot a la hora especificada en el campo `Timestamp` .
`Charge`	El precio que se le cobra por este uso de instancia.
`Version`	La versión de la fuente de datos. La versión posible es la 1.0.

Requisitos del bucket de Amazon S3

Cuando se suscribe a la fuente de datos, debe especificar un bucket de Amazon S3 donde almacenar los archivos de fuente de datos.

Antes de elegir un bucket de Amazon S3 para la fuente de datos, tenga en cuenta lo siguiente:

- Debe tener permisos de `FULL_CONTROL` en ese bucket. Si es el propietario del bucket, tiene este permiso de forma predeterminada. En otro caso, el propietario del bucket debe concederle este permiso a su Cuenta de AWS.
- Cuando se suscriba a una fuente de datos, estos permisos se utilizarán para actualizar la ACL del bucket para conceder el permiso AWS a la cuenta de fuente de datos de `FULL_CONTROL`. La cuenta de fuente de datos de AWS escribe los archivos de fuente de datos en el bucket. Si la cuenta no tiene los permisos necesarios, los archivos de fuente de datos no se pueden escribir en el bucket. Para obtener más información, consulte Registros enviados a Amazon S3 en la Guía del usuario de Registros de Amazon CloudWatch.

> **Note**
>
> Si actualiza la ACL y elimina los permisos de la cuenta de fuente de datos de AWS, los archivos de fuente de datos no se pueden escribir en el bucket. Debe volver a suscribirse a fuente de datos para recibir los archivos de fuente de datos.

- Cada archivo de fuente de datos tiene su propia ACL (independiente de la ACL del bucket). El propietario del bucket tiene permiso `FULL_CONTROL` para los archivos de datos. La cuenta de fuente de datos de AWS tiene permisos de lectura y escritura.
- Si ha aplicado ACL deshabilitadas a sus buckets, agregue una política de bucket que permita a los usuarios con el control total escribir en el bucket. Para obtener más información, consulte Revisar y actualizar políticas de bucket.
- Si elimina su suscripción de fuente de datos, Amazon EC2 no elimina los permisos de lectura y escritura de la cuenta de fuente de datos de AWS ni del bucket ni de los archivos de datos. Debe eliminar esos permisos usted mismo.
- Debe utilizar una clave administrada por el cliente si cifra su bucket de Simple Storage Service (Amazon S3) mediante el cifrado del lado del servidor con una clave AWS KMS almacenada en AWS Key Management Service (SSE-KMS). Para obtener más información, consulte Cifrado del lado del servidor del bucket de Amazon S3 en la Guía del usuario de Amazon CloudWatch Logs.

> **Note**
>
> Para la fuente de datos de instancia de spot, el recurso que genera los archivos S3 ya no son los registros de Amazon CloudWatch. Por lo tanto, debe eliminar la sección `aws:SourceArn` de la política de permisos del bucket de S3 y de la política de KMS.

Suscribirse a su fuente de datos de instancia de spot

Para suscribirse a su fuente de datos, use el comando create-spot-datafeed-subscription.

```
aws ec2 create-spot-datafeed-subscription \
    --bucket my-bucket-name \
    [--prefix my-prefix]
```

Ejemplo de resultado

```
{
    "SpotDatafeedSubscription": {
        "OwnerId": "111122223333",
        "Bucket": "my-bucket-name",
        "Prefix": "my-prefix",
        "State": "Active"
    }
}
```

Describir la fuente de datos de instancias de spot

Para describir la suscripción a la fuente de datos, utilice el comando describe-spot-datafeed-subscription.

```
aws ec2 describe-spot-datafeed-subscription
```

Ejemplo de resultado

```
{
    "SpotDatafeedSubscription": {
        "OwnerId": "123456789012",
        "Prefix": "spotdata",
        "Bucket": "my-s3-bucket",
        "State": "Active"
    }
}
```

Consulta de los datos de su fuente de datos

En la AWS Management Console, abra AWS CloudShell. Use el siguiente comando s3 sync para obtener los archivos .gz del bucket de S3 para su fuente de datos y guárdelos en la carpeta que especifique.

```
aws s3 sync s3://my-s3-bucket ./data-feed
```

Para mostrar el contenido de un archivo .gz, vaya a la carpeta en la que guardó el contenido del bucket de S3.

```
cd data-feed
```

Use el comando ls para ver los nombres de los archivos. Use el comando zcat con el nombre del archivo para mostrar el contenido del archivo comprimido. El siguiente comando es un ejemplo.

```
zcat  111122223333.2023-12-09-07.001.b959dbc6.gz
```

A continuación, se muestra un ejemplo del resultado.

```
#Version: 1.0
#Fields: Timestamp UsageType Operation InstanceID MyBidID MyMaxPrice MarketPrice Charge
 Version
2023-12-09 07:13:47 UTC USE2-SpotUsage:c7a.medium       RunInstances:SV050
 i-0c3e0c0b046e050df     sir-pwq6nmfp    0.0510000000 USD        0.0142000000 USD
  0.0142000000 USD        1
```

Eliminar la fuente de datos de instancia de spot

Para eliminar su fuente de datos, use el comando delete-spot-datafeed-subscription.

```
aws ec2 delete-spot-datafeed-subscription
```

Cuotas de instancias de spot

Existe un límite en la cantidad de instancias de spot en ejecución por Cuenta de AWS por región. Una vez que se cumple una solicitud de instancia de spot pendiente, la solicitud ya no se cuenta para la cuota, ya que la instancia en ejecución se cuenta para la cuota.

Las cuotas de instancias de spot se administran en términos de cantidad de unidades de procesamiento central virtuales (CPU virtuales) que utilizan o utilizarán las instancias de spot en ejecución hasta que se completen las solicitudes de instancia de spot abiertas. Si termina sus instancias de spot, pero no cancela las solicitudes de instancias de spot, las solicitudes se contabilizarán en la cuota de CPU virtuales de su instancia de spot hasta que Amazon EC2 detecte la terminación de las instancias de spot y cierre las solicitudes.

Ofrecemos los siguientes tipos de cuotas para las instancias de spot:

- Todas las solicitudes de instancia de spot DL
- Todas las solicitudes de instancia de spot F
- Todas las solicitudes de instancia de spot G y VT
- Todas las solicitudes de instancia de spot Inf

- Todas las solicitudes de instancia de spot P
- Todas las solicitudes de instancias de spot estándar (A, C, D, H, I, M, R, T, Z)
- Todas las solicitudes de instancias de spot Trn
- Todas las solicitudes de instancia de spot X

Cada tipo de cuota especifica el número máximo de CPU virtuales para una o más familias de instancias. Para obtener información acerca de las diferentes familias, generaciones y tamaños de instancias, consulte Tipos de instancia de Amazon EC2.

Puede iniciar cualquier combinación de tipos de instancias que cumplan las necesidades cambiantes de su aplicación. Por ejemplo, con una cuota de solicitudes de instancias de spot All Standard de 256 CPU virtuales, puede iniciar 32 instancias de spot `m5.2xlarge` (CPU virtuales de 32 x 8) o 16 instancias de spot `c5.4xlarge` (CPU virtuales de 16 x 16).

Tareas

- Monitoreo de las cuotas y el uso de la instancia de spot
- Solicitud de un aumento de cuota.

Monitoreo de las cuotas y el uso de la instancia de spot

Puede ver y administrar las cuotas de sus instancias de spot mediante lo siguiente:

- La página Services Quotas de Amazon EC2 en la consola de Service Quotas
- La AWS CLI get-service-quota

Para obtener más información, consulte Cuotas de servicio de Amazon EC2 y Ver cuotas de servicio en la Guía del usuario de Service Quotas.

Con la integración de métricas de Amazon CloudWatch, puede monitorear el uso de EC2 según sus cuotas. También puede configurar alarmas para recibir advertencias cuando se acerque a las cuotas. Para obtener más información, consulte Service Quotas y alarmas de Amazon CloudWatch en la Guía del usuario de Service Quotas.

Solicitud de un aumento de cuota.

Aunque Amazon EC2 aumenta automáticamente las cuotas de instancias de spot en función del uso, puede solicitar un aumento de la cuota si es necesario. Por ejemplo, si tiene intención de iniciar

más instancias de spot de lo que permite su cuota actual, puede solicitar un aumento de la cuota. También puede solicitar un aumento de la cuota si envía una solicitud de instancia de spot y recibe el error `Max spot instance count exceeded`. Para solicitar un aumento de una cuota, use la consola de Service Quotas, tal como se describe en Cuotas de servicio de Amazon EC2.

Instancias de rendimiento ampliable

Los tipos de instancias T son instancias de rendimiento ampliables. Si inicia instancias de spot mediante un tipo de instancias de rendimiento ampliable y si piensa utilizar instancias de spot de rendimiento ampliable inmediatamente y durante un corto periodo de tiempo, sin tiempo de inactividad para acumular créditos de CPU, le recomendamos que las lance en modo estándar para evitar pagar costos más elevados. Si inicia instancias de spot de rendimiento ampliable en modo ilimitado y amplía el uso de la CPU inmediatamente, gastará créditos sobrantes para el rendimiento ampliable. Si utiliza la instancia durante un periodo corto de tiempo, la instancia no tiene tiempo de acumular créditos de CPU para compensar los créditos sobrantes y se le cobrarán dichos créditos sobrantes al terminar la instancia.

El modo ilimitado resulta adecuado para instancias de spot de rendimiento ampliable solo si la instancia se ejecuta el tiempo suficiente para acumular créditos de CPU para el rendimiento ampliable. De lo contrario, al tener que pagar los créditos sobrantes, las instancias de spot con rendimiento ampliable serán más caras que otras instancias. Para obtener más información, consulte Cuando utilizar el modo ilimitado en lugar del modo de CPU fija.

Las instancias T2, cuando se configuran en modo estándar, obtienen créditos de inicialización. Las instancias T2 son las únicas instancias de rendimiento ampliables que obtienen créditos de inicialización. Los créditos de inicialización tienen como objetivo ofrecer una experiencia de inicialización inicial productiva para instancias T2 proporcionando recursos de computación suficientes para configurar la instancia. No se permiten inicializaciones repetidas de instancias T2 para acceder a nuevos créditos de inicialización. Si necesita una CPU sostenida, puede ganar créditos (mediante un periodo de reposo), utilizar el modo ilimitado para las Instancias de spot T2 o utilizar un tipo de instancia con CPU dedicada.

Dedicated Hosts

Un host dedicado de Amazon EC2 es un servidor físico completamente dedicado para su uso. Si lo desea, puede optar por compartir la capacidad de la instancia con otras cuentas de AWS. Para obtener más información, consulte Utilizar hosts dedicados compartidos.

Los hosts dedicados proporcionan visibilidad y control sobre la ubicación de las instancias y admiten la afinidad de host. Esto significa que puede iniciar y ejecutar instancias en hosts específicos y puede asegurarse de que las instancias se ejecuten solo en hosts específicos. Para obtener más información, consulte Comprender la colocación automática y afinidad.

Los hosts dedicados ofrecen una compatibilidad completa con Traiga su propia licencia (BYOL). Le permiten usar las licencias de software existentes por socket, por núcleo o por VM, entre las que se incluyen Windows Server, SQL Server, SUSE Linux Enterprise Server, Red Hat Enterprise Linux u otras licencias de software que estén vinculadas a VM, sockets o núcleos físicos, según los términos de la licencia.

Si necesita que sus instancias se ejecuten en hardware dedicado, pero no necesita visibilidad ni control sobre la ubicación de las instancias ni tiene que usar licencias de software por socket o por núcleo, puede considerar la posibilidad de usar instancias dedicadas como alternativa. Las instancias dedicadas y los hosts dedicados se pueden utilizar para iniciar instancias de Amazon EC2 en servidores físicos dedicados. No hay diferencias de rendimiento, seguridad o físicas entre las instancias dedicadas y las instancias en hosts dedicados. Sin embargo, hay algunas diferencias clave entre ambos. En la siguiente tabla se enumeran algunas de las principales diferencias entre las instancias dedicadas y los hosts dedicados:

	Host dedicado	Dedicated Instance
Servidor físico dedicado	Servidor físico con capacidad de instancias totalmente dedicado a su uso.	Servidor físico que está dedicado a una sola cuenta de cliente.
Uso compartido de capacidad de instancias	Puede compartir la capacidad de instancias con otras cuentas.	No compatible
Facturación	Facturación por host	Facturación por instancia
Visibilidad de sockets, núcleos e ID de host	Proporciona visibilidad del número de sockets y núcleos físicos	Sin visibilidad

	Host dedicado	Dedicated Instance
Afinidad de instancia y host	Le permite implementar de forma coherente sus instancias en el mismo servidor físico a lo largo del tiempo	No admitido
Colocación de instancia dirigida	Proporciona visibilidad y control adicional sobre el modo en el que las instancias se colocan en un servidor físico	No admitido
Recuperación automática de instancia	Soportado. Para obtener más informaci ón, consulte Recuperación de host.	Compatible
Bring-Your-Own-License (BYOL)	Compatible	Compatibilidad parcial *
Reservas de capacidad	No compatible	Compatible

* Es posible utilizar Microsoft SQL Server con Movilidad de licencias a través de Software Assurance y licencias de Windows Virtual Desktop Access (VDA) con una instancia dedicada.

Para obtener más información sobre instancias dedicadas, consulte Dedicated Instances.

Contenido

- Recuperación de host
- Mantenimiento del host
- Realizar el seguimiento de los cambios de configuración

Configuraciones de capacidad de instancias

Los hosts dedicados admiten diferentes configuraciones (núcleos físicos, sockets y vCPU) que permiten ejecutar instancias de diferentes familias y tamaños.

Al asignar un host dedicado a su cuenta, puede elegir una configuración que admita un tipo de instancia única, o varios tipos de instanciasdentro de la misma familia de instancias. La cantidad de instancias que puede ejecutar en un host depende de la configuración que elija.

Contenido

- Soporte para un solo tipo de instancia
- Compatibilidad con varios tipos de instancias

Soporte para un solo tipo de instancia

Puede asignar un host dedicado que solo admita un tipo de instancia. Con esta configuración, todas las instancias que lance en el host dedicado deben ser del mismo tipo de instancia, el cual especifica al asignar el host.

Por ejemplo, puede asignar un host que solo admita el tipo de instancia `m5.4xlarge`. En este caso, solo puede ejecutar instancias `m5.4xlarge` en ese host.

La cantidad de instancias que puede iniciar en el host depende de la cantidad de núcleos físicos proporcionados por el host y de la cantidad de núcleos consumidos por el tipo de instancia especificado. Por ejemplo, si asigna un host para instancias `m5.4xlarge`, el host proporciona 48 núcleos físicos y cada instancia `m5.4xlarge` consume 8 núcleos físicos. Esto significa que puede iniciar hasta 6 instancias en ese host (48 núcleos físicos/8 núcleos por instancia = 6 instancias).

Compatibilidad con varios tipos de instancias

Puede asignar un host dedicado que admita varios tipos de instancias dentro de la misma familia de instancias. Esto permite ejecutar diferentes tipos de instancias en el mismo host, siempre que estén en la misma familia de instancias y el host tenga suficiente capacidad de instancias.

Por ejemplo, puede asignar un host que admita diferentes tipos de instancias dentro de la familia de instancias R5. En este caso, puede iniciar cualquier combinación de tipos de instancias R5, como `r5.large`, `r5.xlarge`, `r5.2xlarge` y `r5.4xlarge`, en ese host, hasta la capacidad básica física del host.

Las siguientes familias de instancias admiten hosts dedicados que admiten varios tipos de instancias:

- Uso general: A1, M5, M5n, M6i y T3
- Optimizadas para computación: C5, C5n y C6i
- Optimizadas para memoria: R5, R5n y R6i

La cantidad de instancias que puede ejecutar en el host depende de la cantidad de núcleos físicos proporcionados por el host y de la cantidad de núcleos consumidos por cada tipo de instancia que ejecute en el host. Por ejemplo, si asigna un host R5, que proporciona 48 núcleos físicos, y usted ejecuta dos instancias `r5.2xlarge` (4 núcleos x 2 instancias) y tres instancias `r5.4xlarge`(8 núcleos x 3 instancias), esas instancias consumen un total de 32 núcleos y puede ejecutar cualquier combinación de instancias R5 siempre que no superen los 16 núcleos restantes.

Sin embargo, para cada familia de instancias, existe un límite en el número de instancias que se pueden ejecutar para cada tamaño de instancia. Por ejemplo, un host dedicado R5 admite hasta 2 instancias `r5.8xlarge`, lo que utiliza 32 de los núcleos físicos. En este caso, se pueden utilizar instancias R5 adicionales más pequeñas para completar el host hasta la capacidad del núcleo. Para conocer el número de tamaños de instancia admitidos para cada familia de instancias, consulte la Tabla de configuración de hosts dedicados.

En la tabla siguiente se muestran ejemplos de combinaciones de tipos de instancia.

Familia de instancias	Ejemplo de combinaciones de tamaños de instancia	
R5	• Ejemplo 1: 4 x `r5.4xlarge` + 4 x `r5.2xlarge` • Ejemplo 2: 1 x `r5.12xlarge` + 1 x `r5.4xlarge` + 1 x `r5.2xlarge` + 5 x `r5.xlarge` + 2 x `r5.large`	
C5	•	

Familia de instancias	Ejemplo de combinaciones de tamaños de instancia
	Ejemplo 1: 1 x c5.9xlarge + 2 x c5.4xlarge + 1 x c5.xlarge • Ejemplo 2: 4 x c5.4xlarge + 1 x c5.xlarge + 2 x c5.large
M5	• Ejemplo 1: 4 x m5.4xlarge + 4 x m5.2xlarge • Ejemplo 2: 1 x m5.12xlarge + 1 x m5.4xlarge + 1 x m5.2xlarge + 5 x m5.xlarge + 2 x m5.large

Consideraciones

Tenga en cuenta lo siguiente cuando trabaje con servidores dedicados que admitan varios tipos de instancias:

- Con los hosts dedicados de tipo N, como C5n, M5n y R5n, no puede mezclar tamaños de instancia más pequeños (`2xlarge` y más pequeños) con tamaños de instancia más grandes (`4xlarge` y más grande, que incluye `metal`). Si necesita tamaños de instancia más pequeños y más grandes en hosts dedicados de tipo N al mismo tiempo, debe asignar hosts independientes para los tamaños de instancia más pequeños y más grandes.
- Le recomendamos que inicie primero los tipos de instancia más grandes y, a continuación, rellene la capacidad de instancia restante con los tipos de instancia más pequeños según sea necesario.

Bring-Your-Own-License

Los hosts dedicados le permiten utilizar las licencias de software por socket, por núcleo o por máquina virtual. Cuando usa sus propias licencias, es responsable de administrarlas. Sin embargo, Amazon EC2 tiene características que lo ayudan a mantenerse al día con las licencias, como afinidad de instancias y la colocación dirigida.

A continuación se indican los pasos generales que debe seguir para traer su propia imagen de máquina con licencia de volúmenes a Amazon EC2.

1. Compruebe que los términos de la licencia que controlan el uso de sus imágenes de máquinas permiten el uso en un entorno en la nube virtualizado. Para obtener más información acerca de las Licencias de Microsoft, consulte Amazon Web Services and Microsoft Licensing.
2. Después de haber verificado que su imagen de máquina se puede utilizar dentro de Amazon EC2, impórtela utilizando VM Import/Export. Para obtener información acerca de cómo importar su imagen de máquina, consulte la Guía del usuario de VM Import/Export.
3. Después de importar la imagen de máquina, puede iniciar instancias desde ella en los host dedicados activos de la cuenta.
4. Cuando ejecute esas instancias, en función del sistema operativo, es posible que tenga que activarlas con respecto a su propio servidor KMS (por ejemplo, Windows Server o Windows SQL Server). No puede activar las AMI de Windows importadas en el servidor KMS de Windows para Amazon.

> **Note**
>
> Para realizar el seguimiento sobre cómo se usan las imágenes en AWS Config, active el registro de host en AWS. Puede usar AWS Config para registrar los cambios a la configuración de un host dedicado y usar los resultados como origen de datos para los informes de licencias. Para obtener más información, consulte Realizar el seguimiento de los cambios de configuración.

Precios y facturación

El precio de un host dedicado varía según la opción de pago.

Opciones de pago

- Hosts dedicados bajo demanda
- Dedicated Host Reservations
- Savings Plans
- Precios para Windows Server en hosts dedicados

Hosts dedicados bajo demanda

La facturación bajo demanda se activa automáticamente cuando asigna un host dedicado a su cuenta.

El precio bajo demanda de un host dedicado varía por familia de instancias y región. Se paga por segundo (con un mínimo de 60 segundos) por host dedicado activo, independientemente de la cantidad o del tamaño de las instancias que elija iniciar en él. Para obtener más información sobre los precios bajo demanda, consulte Precios bajo demanda de hosts dedicados de Amazon EC2.

Puede liberar un host dedicado bajo demanda en cualquier momento para que deje de acumular cargos. Para obtener información acerca de la liberación de un host dedicado, consulte Liberar hosts dedicados.

Dedicated Host Reservations

Reservas de hosts dedicados proporciona un descuento de facturación en comparación con los hosts dedicados bajo demanda en ejecución. Las reservas están disponibles en tres opciones de pago:

- Sin gastos iniciales— las reservas sin gastos iniciales ofrecen un descuento sobre el uso del host dedicado a lo largo de un plazo y no requieren un pago inicial. Disponible en plazos de uno y tres años. Solo algunas familias de instancias admiten el plazo de tres años para Reservas sin gastos iniciales.
- Pago parcial inicial—: una parte de la reserva se debe pagar de forma anticipada y las demás horas del plazo se facturan con una tarifa con descuento. Disponible en plazos de uno y tres años.
- Pago total anticipado: ofrece el precio efectivo más bajo. Está disponible en plazos de uno y tres años, y cubre todo el costo del gasto inicial del plazo, sin ningún cargo adicional futuro.

Debe tener hosts dedicados activos en la cuenta antes de poder comprar reservas. Cada reserva puede cubrir uno o más hosts compatibles con la misma familia de instancias en una única zona de disponibilidad. Las reservas se aplican a la familia de instancias en el host y no al tamaño de la instancia. Si tiene tres hosts dedicados con diferentes tamaños de instancias (`m4.xlarge`, `m4.medium` y `m4.large`), puede asociar una única reserva de `m4` con todos esos hosts dedicados. La familia de instancias y la zona de disponibilidad de la reserva deben coincidir con las de los hosts dedicados con los que desea asociarla.

Cuando hay una reserva asociada con un host dedicado, no se podrá liberar dicho host dedicado hasta que finalice el plazo de la reserva.

Para obtener más información acerca de los precios de reserva, consulte la página Precios de hosts dedicados de Amazon EC2.

Savings Plans

Los Savings Plans son un modelo flexible de precios que ofrece ahorros significativos sobre los instancias bajo demanda. Con los Savings Plans, se compromete a una cantidad de uso constante, en USD por hora, durante un período de 1 o 3 años. Esto le proporciona la flexibilidad para usar los hosts dedicados que mejor satisfagan sus necesidades y continúe ahorrando dinero, en lugar de comprometerse con un host dedicado específico. Para obtener más información, consulte la Guía del usuario de Savings Plans de AWS.

> **Note**
>
> Los Savings Plans no se admiten con los hosts dedicados `u-6tb1.metal`, `u-9tb1.metal`, `u-12tb1.metal`, `u-18tb1.metal` `yu-24tb1.metal`.

Precios para Windows Server en hosts dedicados

Sujetos a los términos de licencia de Microsoft, puede llevar las licencias existentes de Windows Server y SQL Server a hosts dedicados. No hay cargo adicional por el uso de software si elije traer sus propias licencias.

Además, también puede utilizar las AMI de Windows Server que proporciona Amazon para ejecutar las versiones más recientes de Windows Server en hosts dedicados. Esto es común para escenarios en los que tiene licencias de SQL Server existentes elegibles para ejecutarse en hosts dedicados pero requieren Windows Server para ejecutar la carga de trabajo de SQL Server. Las AMI de Windows Server proporcionadas por Amazon solo se admiten en los tipos de instancia de generación actual. Para obtener más información, consulte Precios de hosts dedicados de Amazon EC2.

instancias T3 ampliables en hosts dedicados

Los hosts dedicados admiten instancias T3 de rendimiento ampliable. Las instancias T3 proporcionan una forma rentable de utilizar el software de licencia elegible BYOL en equipo dedicado. La menor huella de vCPU de las instancias T3 permite consolidar sus cargas de trabajo en menos hosts y maximizar la utilización de licencias por núcleo.

Los hosts dedicados T3 son los más adecuados para ejecutar el software BYOL con una utilización de CPU baja a moderada. Esto incluye las licencias de software aptas por socket, por núcleo o por

software VM, como Windows Server, Windows Desktop, SQL Server, SUSE Enterprise Linux Server, Red Hat Enterprise Linux y Oracle Database. Entre los ejemplos de cargas de trabajo adecuadas para los hosts dedicados T3 se incluyen las bases de datos pequeñas y medianas, escritorios virtuales, entornos de desarrollo y pruebas, repositorios de código y prototipos de productos. No se recomiendan los hosts dedicados T3 para cargas de trabajo con una utilización sostenida de CPU elevada o para cargas de trabajo que experimentan ampliaciones de CPU correlacionadas simultáneamente.

Las instancias T3 en hosts dedicados utilizan el mismo modelo de crédito que las instancias T3 en equipo de tenencia compartida. Sin embargo, solo admiten el modo de crédito `standard`; no admiten el modo de crédito `unlimited`. En el modo `standard`, las instancias T3 de hosts dedicados ganan, gastan y acumulan créditos de la misma manera que las instancias ampliables en hardware de tenencia compartida. Proporcionan un rendimiento básico de CPU con la capacidad de ampliarse por encima del nivel básico. Para ampliar por encima de la base de referencia, la instancia gasta créditos que ha acumulado en su saldo de créditos de CPU. Cuando se agotan los créditos acumulados, la utilización de CPU se reduce al nivel de básico. Para obtener más información sobre el modo `standard`, consulte Cómo funcionan las instancias de rendimiento ampliable estándar.

Los hosts dedicados T3 admiten todas las características que ofrecen los hosts dedicados de Amazon EC2, como varios tamaños de instancias en un solo host, grupos de recursos de host y BYOL.

Tamaños y configuraciones de instancias T3 admitidos

Los hosts dedicados T3 ejecutan instancias T3 ampliables de uso general que comparten recursos de CPU del host, al proporcionar un rendimiento básico de CPU y la capacidad de ampliarse a un nivel más alto cuando sea necesario. Esto permite que los hosts dedicados T3, que tienen 48 núcleos, puedan admitir hasta un máximo de 192 instancias por host. Con el fin de utilizar eficientemente los recursos del host y proporcionar el mejor rendimiento de la instancia, el algoritmo de colocación de las instancias de Amazon EC2 calcula de manera automática el número admitido de instancias y combinaciones de tamaño de instancia que se pueden iniciar en el host.

Los hosts dedicados T3 admiten varios tipos de instancias en el mismo host. En los hosts dedicados, se admiten todos los tamaños de las instancias T3. Puede ejecutar diferentes combinaciones de instancias T3 hasta el límite de CPU del host.

En la siguiente tabla, se enumeran los tipos de instancias admitidos, se resume el rendimiento de cada tipo de instancias y se indica el número máximo de instancias de cada tamaño que se pueden iniciar.

Tipo de insta	vCPU	Memoria (GiB)	Utilización de CPU de referencia por vCPU	Banda ancha con ampliación de red (Gbps)	Banda ancha con ampliación de Amazon EBS (Mbps)	Número máximo de instancias por host dedicado
t3.na	2	0,5	5%	5	Hasta 2085	192
t3.m	2.	1	10%	5	Hasta 2085	192
t3.sn	2	2.	20%	5	Hasta 2085	192
t3.m	2	4	20%	5	Hasta 2085	192
t3.la	2	8	30%	5	2780	96
t3.xl	4	16	40 %	5	2780	48
t3.2x e	8	32	40 %	5	2780	24

Monitorear la utilización de CPU para los hosts dedicados T3

Puede utilizar la métrica de Amazon CloudWatch `DedicatedHostCPUUtilization` para monitorear la utilización de las vCPU de un host dedicado. La métrica se encuentra disponible en el espacio de nombres `EC2` y la dimensión `Per-Host-Metrics`. Para obtener más información, consulte Métricas de host dedicado.

Restricciones de los hosts dedicados

Antes de asignar los hosts dedicados, recuerde las siguientes limitaciones y restricciones:

- Para ejecutar RHEL, SUSE Linux y SQL Server en hosts dedicados, debe traer sus propias AMI. Las AMI de RHEL, SUSE Linux y SQL Server que ofrece AWS o que están disponibles en AWS Marketplace no se pueden utilizar con los hosts dedicados. Para obtener más información sobre cómo crear su propia AMI, consulte Bring-Your-Own-License.

  Esta restricción no se aplica a los hosts asignados para instancias de memoria alta (`u-6tb1.metalu-9tb1.metal`, `u-12tb1.metal`, `u-18tb1.metal` y `u-24tb1.metal`).

Las AMI RHEL y SUSE Linux que ofrece AWS o que están disponibles en AWS Marketplace se pueden utilizar con estos hosts.

- Existe un límite en la cantidad de hosts dedicados en ejecución según la familia de instancias por cuenta de AWS por región. Las cuotas se aplican solo a las instancias en ejecución. Si su instancia está pendiente, en proceso de detención o detenida, no se tendrá en cuenta para su cuota. Para ver las cuotas de la cuenta o solicitar un aumento de una cuota, use la consola de Service Quotas.
- Las instancias que se ejecutan en un host dedicado solo se pueden iniciar en una VPC.
- Los grupos de Auto Scaling solo se admiten cuando se usa una plantilla de inicialización que especifica un grupo de recursos del host. Para obtener más información, consulte Crear una plantilla de lanzamiento mediante la configuración avanzada en la Guía del usuario de Amazon EC2 Auto Scaling.
- No se admiten instancias de Amazon RDS.
- La capa de uso gratuita de AWS no está disponible para los hosts dedicados.
- El control de ubicación de instancias hace referencia a la administración de inicializacións de instancias en los hosts dedicados. No se pueden iniciar hosts dedicados en grupos de ubicación.
- Si asigna un host a un tipo de instancia virtualizada, no podrá modificar el tipo de instancia al tipo `.metal` después de asignar el host. Por ejemplo, si asigna un host al tipo de instancia `m5.large`, no podrá modificar el tipo de instancia a `m5.metal`.

  De modo similar, si asigna un host a un tipo de instancia `.metal`, no podrá modificar el tipo de instancia al tipo virtualizada después de asignar el host. Por ejemplo, si asigna un host al tipo de instancia `m5.metal`, no podrá modificar el tipo de instancia a `m5.large`.

Utilizar hosts dedicados

Para usar un host dedicado, primero debe asignar hosts para su uso en la cuenta. A continuación, inicia instancias en los hosts especificando la tenencia de host para la instancia. Debe seleccionar un host específico para la instancia en la que iniciar o puede permitir iniciar en cualquier host que tenga habilitada la colocación automática y coincida con su tipo de instancia. Cuando una instancia se detiene y se reinicia, la configuración de afinidad de hosts determina si se reinicia en el mismo host o en uno diferente.

Si ya no necesita un host bajo demanda, puede detener las instancias que se ejecutan en el host, dirigirlas para iniciarlas en un host distinto y, a continuación, liberar el host.

Los hosts dedicados también se integran con AWS License Manager. Con License Manager, puede crear un grupo de recursos de host, que es una colección de hosts dedicados que se administran como una sola entidad. Al crear un grupo de recursos de host, especifique las preferencias de administración de host, como la asignación automática y las versiones automáticas, para los hosts dedicados. Esto le permite iniciar instancias en hosts dedicados sin asignar y administrar manualmente esos hosts. Para obtener más información, consulte Grupos de recursos de host en la Guía del usuario de AWS License Manager.

Contenido

Asignar hosts dedicados

Para empezar a usar hosts dedicados, debe asignar hosts dedicados a su cuenta desde la consola de Amazon EC2 o las herramientas de línea de comandos. Después de asignar el host dedicado, la capacidad del host dedicado está disponible inmediatamente en la cuenta y ya puede empezar a iniciar instancias en el host dedicado.

Al asignar un host dedicado a su cuenta, puede elegir una configuración que admita un tipo de instancia única, o varios tipos de instanciasdentro de la misma familia de instancias. La cantidad de instancias que puede ejecutar en el host depende de la configuración que elija. Para obtener más información, consulte Configuraciones de capacidad de instancias.

Console

Para asignar un host dedicado

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Dedicated Hosts (Hosts dedicados) y, a continuación, elija Allocate Dedicated Host (Asignar host dedicado).
3. Para Instance family (Familia de instancias), elija la familia de instancias para el host dedicado.
4. Especifique si el host dedicado admite múltiples tamaños de instancia dentro de la familia de instancias seleccionada o solo un tipo de instancia específico. Aplique alguna de las siguientes acciones.
   - Para configurar el host dedicado para que admita distintos tipos de instancia en la familia de instancias seleccionada, para Support multiple instance types (Compatibilidad con varios tipos de instancia), elija Enable (Habilitar). Al activar esto, puede iniciar distintos tamaños de instancia desde la misma familia de instancias en el host dedicado. Por ejemplo, si elige la familia de instancias `m5` y opta por esta opción, puede iniciar las instancias `m5.xlarge` y `m5.4xlarge` en el host dedicado.
   - Para configurar el host dedicado para que admita un tipo de instancia único dentro de la familia de instancias seleccionada, vacíe Support multiple instance types (Compatibilidad con varios tipos de instancia) y, luego, para Instance type (Tipo de instancia), elija el tipo de instancia que debe ser compatible. Esto le permite iniciar un único tipo de instancia en el host dedicado. Por ejemplo, si elige esta opción y especifica `m5.4xlarge` como el tipo de instancias admitido, únicamente podrá iniciar instancias `m5.4xlarge` en el host dedicado.
5. En Availability Zone (Zona de disponibilidad), seleccione la zona de disponibilidad en la que desea asignar el host dedicado.
6. Para permitir que el host dedicado acepte inicializacións de instancias sin destino que coincidan con su tipo de instancia, en Instance auto-placement (Permitir colocación automática de instancia), elija Enable (Habilitar). Para obtener más información acerca de la colocación automática, consulte Comprender la colocación automática y afinidad.
7. Para habilitar la recuperación del host para el host dedicado, en Host recovery (Recuperación del host) elija Enable (Habilitar). Para obtener más información, consulte Recuperación de host.
8. Para Quantity (Cantidad), indique el número de hosts dedicados que desea asignar.

9. (Opcional) Elija Add new tag (Agregar nueva etiqueta) y especifique una clave y un valor de la etiqueta.
10. Elija Allocate.

AWS CLI

Para asignar un host dedicado

Utilice el comando de la AWS CLI allocate-hosts. Los siguientes comandos asignan un host dedicado que admite múltiples tipos de instancia desde la familia de instancias `m5` en la zona de disponibilidad `us-east-1a`. El host también tiene habilitada la recuperación del host y tiene la colocación automática desactivada.

```
aws ec2 allocate-hosts --instance-family "m5" --availability-zone "us-east-1a" --
auto-placement "off" --host-recovery "on" --quantity 1
```

Los siguientes comandos asignan un host dedicado que admite inicializacións de instancias sin destino `m4.large` en la zona de disponibilidad `eu-west-1a`, habilita la recuperación del host y aplica una etiqueta con una clave de `purpose` y un valor de `production`.

```
aws ec2 allocate-hosts --instance-type "m4.large" --availability-zone "eu-west-1a"
 --auto-placement "on" --host-recovery "on" --quantity 1 --tag-specifications
 'ResourceType=dedicated-host,Tags=[{Key=purpose,Value=production}]'
```

PowerShell

Para asignar un host dedicado

Utilice el comando AWS Tools for Windows PowerShell New-EC2Host. Los siguientes comandos asignan un host dedicado que admite múltiples tipos de instancia desde la familia de instancias `m5` en la zona de disponibilidad `us-east-1a`. El host también tiene habilitada la recuperación del host y tiene la colocación automática desactivada.

```
PS C:\> New-EC2Host -InstanceFamily m5 -AvailabilityZone us-east-1a -
AutoPlacement Off -HostRecovery On -Quantity 1
```

Los siguientes comandos asignan un host dedicado que admite inicializacións de instancias sin destino `m4.large` en la zona de disponibilidad `eu-west-1a`, habilitan la recuperación del host y aplican una etiqueta con una clave de `purpose` y un valor de `production`.

El parámetro `TagSpecification` utilizado para etiquetar un host dedicado en la creación requiere un objeto que especifique el tipo de recurso que se va a etiquetar, la clave de etiqueta y el valor de etiqueta. Los siguientes comandos crean el objeto necesario.

```
PS C:\> $tag = @{ Key="purpose"; Value="production" }
PS C:\> $tagspec = new-object Amazon.EC2.Model.TagSpecification
PS C:\> $tagspec.ResourceType = "dedicated-host"
PS C:\> $tagspec.Tags.Add($tag)
```

El siguiente comando asignar el host dedicado y aplica la etiqueta especificada en el objeto `$tagspec`.

```
PS C:\> New-EC2Host -InstanceType m4.large -AvailabilityZone eu-west-1a -
AutoPlacement On -HostRecovery On -Quantity 1 -TagSpecification $tagspec
```

iniciar instancias en un host dedicado

Después de asignar un host dedicado, puede iniciar instancias en él. No puede iniciar instancias con la tenencia de `host` si no tiene hosts dedicados activos con suficiente capacidad disponible para el tipo de instancia que va a iniciar.

> **Tip**
>
> En el caso de los hosts dedicados que admiten varios tamaños de instancia, le recomendamos que inicie primero los tamaños de instancia más grandes y, a continuación, rellene la capacidad de instancia restante con los tamaños de instancia más pequeños según sea necesario.

Antes de iniciar las instancias, tenga en cuenta las limitaciones. Para obtener más información, consulte Restricciones de los hosts dedicados.

Puede iniciar una instancia en un host dedicado utilizando los siguientes métodos.

Console

Para iniciar una instancia en un host dedicado específico desde la página de hosts dedicados

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

2. En el panel de navegación, seleccione Dedicated Hosts (Hosts dedicados).
3. En la página Dedicated Hosts (Hosts dedicados), seleccione un host y haga clic en Actions (Acciones), Launch Instance(s) onto host (iniciar instancias en el host).
4. En la sección Application and OS Images (Imágenes de aplicaciones y sistema operativo), seleccione una AMI en la lista.

   > **Note**
   >
   > Las AMI de SQL Server, SUSE y RHEL que proporciona Amazon EC2 no se pueden utilizar con hosts dedicados.

5. En la sección Instance type (Tipo de instancia), seleccione un tipo de instancia para iniciarla.

   > **Note**
   >
   > Si el host dedicado admite solo un tipo de instancia, el tipo de instancia admitido se selecciona de forma predeterminada y no se puede modificar.
   > Si el host dedicado admite varios tipos de instancia, debe seleccionar un tipo de instancia de la familia de instancias admitida en función de la capacidad de la instancia disponible del host dedicado. Le recomendamos que inicie primero los tamaños de instancia más grandes y, a continuación, rellene la capacidad de instancia restante con los tamaños de instancia más pequeños según sea necesario.

6. En la sección Key pair (Par de claves), seleccione el par de claves para asociarlo con la instancia.
7. En la sección Advanced details (Detalles avanzados), en Tenancy affinity (Afinidad de la tenencia), lleve a cabo una de las siguientes acciones:

   - Seleccione Off (Apagada): la instancia se inicia en el host específico pero, si la instancia se detiene, no está garantizado que se reinicie en el mismo host dedicado.
   - Seleccione el ID de host dedicado: si se detiene, la instancia siempre se reinicia en este host específico.

   Para obtener más información acerca de la afinidad, consulte Comprender la colocación automática y afinidad.

> **Note**
>
> Las opciones Tenancy (Tenencia) y Host están preconfiguradas en función del host que haya seleccionado.

8. Configure las opciones de instancia restantes según sea necesario. Para obtener más información, consulte iniciar una instancia mediante parámetros definidos.
9. Seleccione iniciar instancia.

Para iniciar una instancia en un host dedicado utilizando el launch wizard de instancias

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione instancias y elija iniciar instancia.
3. En la sección Application and OS Images, seleccione una AMI en la lista.

> **Note**
>
> Las AMI de SQL Server, SUSE y RHEL que proporciona Amazon EC2 no se pueden utilizar con hosts dedicados.

4. En la sección Instance type, seleccione un tipo de instancia para iniciarla.
5. En la sección Key pair, seleccione el par de claves para asociarlo con la instancia.
6. En la sección Detalles avanzados, haga lo siguiente:
   a. En Tenancy (Tenencia), seleccione Dedicated host (Host dedicado).
   b. En Target host by (Host de destino por), seleccione Host ID (ID de host).
   c. En Target host ID (ID de host de destino), seleccione el host en el que se va a iniciar la instancia.
   d. En Tenancy affinity (Afinidad de tenencia), lleve a cabo una de las siguientes acciones:
      - Seleccione Off (Apagada): la instancia se inicia en el host específico pero, si la instancia se detiene, no está garantizado que se reinicie en el mismo host dedicado.
      - Seleccione el ID de host dedicado: si se detiene, la instancia siempre se reinicia en este host específico.

Para obtener más información acerca de la afinidad, consulte Comprender la colocación automática y afinidad.

7. Configure las opciones de instancia restantes según sea necesario. Para obtener más información, consulte iniciar una instancia mediante parámetros definidos.
8. Seleccione iniciar instancia.

AWS CLI

Para iniciar una instancia en un host dedicado

Utilice el comando de la AWS CLI run-instances y especifique la afinidad de instancia, la tenencia y el host en el parámetro de la solicitud `Placement`.

PowerShell

Para iniciar una instancia en un host dedicado

Utilice el comando de AWS Tools for Windows PowerShell New-EC2Instance y especifique la afinidad, la tenencia y el host de instancia en el parámetro de la solicitud `Placement`.

iniciar instancias en un grupo de recursos de host

Cuando inicia una instancia en un grupo de recursos de host que tiene un host dedicado con capacidad de instancia disponible, Amazon EC2 inicia la instancia en ese host. Si el grupo de recursos de host no tiene un host con capacidad de instancia disponible, Amazon EC2 asigna automáticamente un nuevo host en el grupo de recursos de host y, a continuación, inicia la instancia en ese host. Para obtener más información, consulte Grupos de recursos de host en la Guía del usuario de AWS License Manager.

Requisitos y límites

- Debe asociar una configuración de licencia basada en núcleo o conector con la AMI.
- No puede utilizar las AMI de SQL Server, SUSE o RHEL proporcionadas por Amazon EC2 en hosts dedicados.
- No se puede establecer el host de destino eligiendo un ID de host y no se puede habilitar la afinidad de instancias al iniciar una instancia en un grupo de recursos de host.

Puede iniciar una instancia en un grupo de recursos de host utilizando los siguientes métodos.

Console

Para iniciar una instancia en un grupo de recursos de host

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione instancias y elija iniciar instancia.
3. En la sección Application and OS Images, seleccione una AMI en la lista.

   > **Note**
   >
   > Las AMI de SQL Server, SUSE y RHEL que proporciona Amazon EC2 no se pueden utilizar con hosts dedicados.

4. En la sección Instance type, seleccione un tipo de instancia para iniciarla.
5. En la sección Key pair, seleccione el par de claves para asociarlo con la instancia.
6. En la sección Detalles avanzados, haga lo siguiente:

   a. En Tenancy (Tenencia), seleccione Dedicated host (Host dedicado).

   b. En Target host by (Host de destino por), seleccione Host resource group (Grupo de recursos de host).

   c. En Tenancy host resource group (Grupo de recursos de host de tenencia), seleccione el grupo de recursos de host en el que se va a iniciar la instancia.

   d. En Tenancy affinity, lleve a cabo una de las siguientes acciones:

      - Seleccione Off (Apagada): la instancia se inicia en el host específico pero, si la instancia se detiene, no está garantizado que se reinicie en el mismo host dedicado.
      - Seleccione el ID de host dedicado: si se detiene, la instancia siempre se reinicia en este host específico.

      Para obtener más información acerca de la afinidad, consulte Comprender la colocación automática y afinidad.

7. Configure las opciones de instancia restantes según sea necesario. Para obtener más información, consulte iniciar una instancia mediante parámetros definidos.
8. Seleccione iniciar instancia.

AWS CLI

Para iniciar una instancia en un grupo de recursos de host

Utilice el comando de la AWS CLI run-instances y, en el parámetro de la solicitud `Placement`, omita la opción Tenancy y especifique el ARN del grupo de recursos de host.

PowerShell

Para iniciar una instancia en un grupo de recursos de host

Utilice el comando de AWS Tools for Windows PowerShell New-EC2Instance y, en el parámetro de la solicitud `Placement`, omita la opción Tenancy y especifique el ARN del grupo de recursos de host.

Comprender la colocación automática y afinidad

El control de la ubicación para los hosts dedicados se realiza tanto en el nivel de la instancia como en el nivel del host.

Colocación automática

La colocación automática debe configurarse en el nivel de host. Además, permite administrar si las instancias se inician en un host específico o en cualquier host disponible con una configuración coincidente.

Cuando la colocación automática de un host dedicado está deshabilitada, solo acepta inicializacións de instancias con tenencia de Host que especifiquen el ID de host único. Esta es la configuración predeterminada para los nuevos hosts dedicados.

Cuando la colocación automática de un host dedicado está habilitada, acepta cualquier inicialización de instancia sin destino que coincida con su configuración de tipo de instancia.

Al iniciar una instancia, tiene que configurar su tenencia. la inicialización de una instancia en un host dedicado sin proporcionar un `HostId` específico, permite la inicialización en cualquier host dedicado que tenga la colocación automática habilitada y coincida con su tipo de instancia.

Afinidad de hosts

La afinidad de host está configurada en el nivel de instancia. Establece una relación de inicialización entre una instancia y un host dedicado.

Cuando la afinidad se establece en `Host`, si una instancia iniciada en un host específico se detiene, siempre se reiniciará en el mismo host. Esto se aplica tanto a los inicializacións con destino como sin destino.

Cuando la afinidad está establecida en `Default` y usted para y reinicia la instancia, esta se puede reiniciar en cualquier host disponible. Sin embargo, intentará volver a iniciarse en el último host dedicado en el que se haya ejecutado (dentro de lo posible).

Modificar la ubicación automática del host dedicado

Puede modificar la configuración de colocación automática de un host dedicado después de asociarlo a su cuenta de AWS, utilizando uno de los siguientes métodos.

Console

Para modificar la colocación automática de un host dedicado

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Hosts dedicados (Hosts dedicados).
3. Seleccione un host y elija Actions (Acciones), Modify host (Modificar host).
4. En Instance auto-placement (instancias de colocación automática), elija Enable (Habilitar) para habilitar la colocación automática o desactive Enable (Habilitar) para deshabilitar la colocación automática. Para obtener más información, consulte Comprender la colocación automática y afinidad.
5. Seleccione Guardar.

AWS CLI

Para modificar la colocación automática de un host dedicado

Utilice el comando de la AWS CLI modify-hosts. En los ejemplos siguientes se habilita la colocación automática del host dedicado especificado.

```
aws ec2 modify-hosts --auto-placement on --host-ids h-012a3456b7890cdef
```

PowerShell

Para modificar la colocación automática de un host dedicado

Utilice el comando de AWS Tools for Windows PowerShell Edit-EC2Host. En los ejemplos siguientes se habilita la colocación automática del host dedicado especificado.

```
PS C:\> Edit-EC2Host --AutoPlacement 1 --HostId h-012a3456b7890cdef
```

Modificar los tipos de instancia admitidos

La compatibilidad con varios tipos de instancia en el mismo host dedicado está disponible para las siguientes familias de instancias: C5, M5, R5, C5n, R5n, M5n y T3. Otras familias de instancias solo admiten un único tipo de instancia en el mismo host dedicado.

Puede asignar un host dedicado utilizando los métodos siguientes.

Puede modificar un host dedicado para cambiar los tipos de instancia que admite. Si actualmente admite un tipo de instancia individual, puede modificarlo para que admita varios tipos de instancia dentro de la familia de instancias. De similar modo, si actualmente admite varios tipos de instancia, puede modificarlo para que solo admita un tipo de instancia específico.

Para modificar un host dedicado para que admita los tipos de instancia, primero debe detener todas las instancias en ejecución en el host. La modificación puede tardar aproximadamente 10 minutos en completarse. El host dedicado pasa a tener el estado `pending` mientras la modificación esté en proceso. No puede detener las instancias paradas ni iniciar instancias nuevas en host dedicado mientras tenga el estado `pending`.

Para modificar un host dedicado que admite varios tipos de instancia para que admita solo un tipo de instancia único, el host o bien no puede tener instancias en ejecución o bien dichas instancias deben ser del tipo de instancia que quiere que admita el host. Por ejemplo, para modificar un host que admite varios tipos de instancia en la familia de instancias `m5` para que solo admita instancias `m5.large`, el host dedicado debe o bien ejecutar las instancias en ejecución o solo ejecutar instancias `m5.large`.

Si asigna un host a un tipo de instancia virtualizada, no podrá modificar el tipo de instancia al tipo `.metal` después de asignar el host. Por ejemplo, si asigna un host al tipo de instancia `m5.large`, no podrá modificar el tipo de instancia a `m5.metal`. De modo similar, si asigna un host a un tipo de instancia `.metal`, no podrá modificar el tipo de instancia al tipo virtualizada después de asignar el host. Por ejemplo, si asigna un host al tipo de instancia `m5.metal`, no podrá modificar el tipo de instancia a `m5.large`.

Puede modificar los tipos de instancia admitidos mediante uno de los métodos siguientes.

Console

Para modificar los tipos de instancia admitidos para un host dedicado

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Dedicated Host (Host dedicado).
3. Seleccione el host dedicado que desea modificar y elija Actions (Acciones), Modify host (Modificar host).
4. Lleve a cabo una de las siguientes acciones, en función de la configuración actual del host dedicado:

   - Si host dedicado actualmente admite un tipo de instancia específico, Support multiple instance types (Compatibilidad con múltiples tipos de instancias) no está habilitado e Instance type (Tipo de instancia) muestra el tipo de instancia admitido. Para modificar el host para que admita varios tipos de instancia en la familia de instancias actual, en Support multiple instance types (Compatibilidad con múltiples tipos de instancia), elija Enable (Habilitar).

     Antes de modificar el host para que admita varios tipos de instancia, primero debe detener todas las instancias en ejecución en el host.
   - Si host dedicado actualmente admite varios tipos de instancia en una familia de instancias, Enabled (Habilitado) está seleccionado para Support multiple instance types (Compatibilidad con varios tipos de instancia). Para modificar el host para que admita un tipo de instancia específico, en Support multiple instance types (Compatibilidad con varios tipos de instancia), desactive Enable (Habilitar) y, a continuación, en Instance type (Tipo de instancia), seleccione el tipo de instancia concreto que desea admitir.

     No se puede modificar la familia de instancias admitida por el host dedicado.
5. Seleccione Guardar.

AWS CLI

Para modificar los tipos de instancia admitidos para un host dedicado

Utilice el comando de la AWS CLI modify-hosts.

El siguiente comando modifica un host dedicado para admitir varios tipos de instancia en la familia de instancias `m5`.

```
aws ec2 modify-hosts --instance-family m5 --host-ids h-012a3456b7890cdef
```

El siguiente comando modifica un host dedicado para admitir solo instancias `m5.xlarge`.

```
aws ec2 modify-hosts --instance-type m5.xlarge --instance-family --host-
ids h-012a3456b7890cdef
```

PowerShell

Para modificar los tipos de instancia admitidos para un host dedicado

Utilice el comando de AWS Tools for Windows PowerShell Edit-EC2Host.

El siguiente comando modifica un host dedicado para admitir varios tipos de instancia en la familia de instancias `m5`.

```
PS C:\> Edit-EC2Host --InstanceFamily m5 --HostId h-012a3456b7890cdef
```

El siguiente comando modifica un host dedicado para admitir solo instancias `m5.xlarge`.

```
PS C:\> Edit-EC2Host --InstanceType m5.xlarge --HostId h-012a3456b7890cdef
```

Modificar la tenencia y la afinidad de una instancia

Puede cambiar la tenencia de una instancia después de haberla iniciado. También puede modificar la afinidad de la instancia para que se dirija a un host específico o permitir que se lance en cualquier host dedicado disponible con atributos coincidentes en su cuenta. Para modificar la tenencia o la afinidad de la instancia, la instancia debe tener el estado `stopped`.

Los detalles del sistema operativo de la instancia (y si SQL Server está instalado) influyen en las conversiones que se admiten. Para obtener más información sobre las rutas de conversión de tenencia disponibles para su instancia, consulte Tenancy conversion en la Guía del usuario de License Manager.

> **Note**
>
> En el caso de las instancias T3, debe iniciar la instancia en un host dedicado para poder utilizar una tenencia de `host`. En el caso de las instancias T3, no se puede cambiar la

tenencia de `host` a `dedicated` o `default`. Al intentar realizar uno de estos cambios de tenencia no admitidos, se produce el código de error `InvalidRequest`.

Puede modificar la tenencia y la afinidad de una instancia mediante los métodos siguientes.

Console

Para modificar la tenencia o afinidad de instancias

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. Elija Instances (instancia[s]) y, a continuación, seleccione la instancia que desee modificar.
3. Elija Instance state (Estado de la instancia) y Stop (Detener).
4. Con la instancia aún seleccionada, elija Acciones, Configuración de la instancia, Cambiar ubicación de la instancia.
5. En la página Modificar ubicación de instancia, configure lo siguiente:

   - Tenancy (Tenencia): elija una de las siguientes opciones:
     - Run a dedicated hardware instance (Ejecutar como instancia de hardware dedicada): inicia la instancia como una instancia dedicada. Para obtener más información, consulte Dedicated Instances.
     - Launch the instance on a host dedicado (iniciar la instancia en un host dedicado): inicia la instancia en un host dedicado con afinidad configurable.
   - Affinity (Afinidad): elija una de las siguientes opciones:
     - This instance can run on any one of my hosts (La instancia se puede ejecutar en cualquiera de mis hosts): la instancia se inicia en cualquier host dedicado disponible de su cuenta que admita su tipo de instancia.
     - This instance can only run on the selected host (Esta instancia solo se puede ejecutar en el host seleccionado): la instancia solo se puede ejecutar en el host dedicado seleccionado para Target Host (Host de destino).
   - Target Host (Host de destino)—: seleccione el host dedicado donde se debe ejecutar la instancia. Si no se muestra ningún host de destino, es posible que no tenga disponible, ningún host dedicado compatible en su cuenta.

   Para obtener más información, consulte Comprender la colocación automática y afinidad.

6. Seleccione Save.

AWS CLI

Para modificar la tenencia o afinidad de instancias

Utilice el comando de la AWS CLI modify-instance-placement. En los ejemplos siguientes se cambia la afinidad de la instancia especificada de `default` a `host` y se especifica el host dedicado con el que tiene afinidad la instancia.

```
aws ec2 modify-instance-placement --instance-id i-1234567890abcdef0 --affinity host
 --tenancy host --host-id h-012a3456b7890cdef
```

PowerShell

Para modificar la tenencia o afinidad de instancias

Utilice el comando de AWS Tools for Windows PowerShell Edit-EC2InstancePlacement. En los ejemplos siguientes se cambia la afinidad de la instancia especificada de `default` a `host` y se especifica el host dedicado con el que tiene afinidad la instancia.

```
PS C:\> Edit-EC2InstancePlacement -InstanceId i-1234567890abcdef0 -Affinity host -
Tenancy host -HostId h-012a3456b7890cdef
```

Ver hosts dedicados

Puede ver detalles sobre un host dedicado y las instancias individuales que este contiene mediante los métodos siguientes.

Console

Para ver los detalles de un host dedicado

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Hosts dedicados (Hosts dedicados).
3. En la página Dedicated Hosts (Hosts dedicados), seleccione un host.
4. Para obtener información sobre el host, elija Details (Detalles).

Available vCPUs (vCPU disponibles) indica los vCPU disponibles en host dedicado para los inicializacións de instancias nuevas. Por ejemplo, un host dedicado que admite varios tipos de instancia en la familia de instancias `c5` y en el que no se ejecutan instancias, tiene 72 vCPU disponibles. Esto significa que puede iniciar distintas combinaciones de tipos de instancia en el host dedicado para consumir los 72 vCPU disponibles.

Para obtener información sobre las instancias que se ejecutan en el host, elija Running instances (instancias en ejecución).

AWS CLI

Para ver la capacidad de un host dedicado

Utilice el comando de la AWS CLI describe-hosts.

En el siguiente ejemplo se emplea el comando describe-hosts (AWS CLI) para ver la capacidad disponible de la instancia para un host dedicado que admite varios tipos de instancias de la familia de instancias `c5`. En el host dedicado ya se ejecutan dos instancias `c5.4xlarge` y cuatro instancias `c5.2xlarge`.

```
aws ec2 describe-hosts --host-id h-012a3456b7890cdef
```

```
"AvailableInstanceCapacity": [
    { "AvailableCapacity": 2,
      "InstanceType": "c5.xlarge",
      "TotalCapacity": 18 },
    { "AvailableCapacity": 4,
      "InstanceType": "c5.large",
      "TotalCapacity": 36 }
  ],
"AvailableVCpus": 8
```

PowerShell

Para ver la capacidad de instancia de un host dedicado

Utilice el comando de AWS Tools for Windows PowerShell Get-EC2Host.

```
PS C:\> Get-EC2Host -HostId h-012a3456b7890cdef
```

Etiquetar hosts dedicados

Puede asignar etiquetas personalizadas a sus host dedicados existentes para clasificarlos de diversas maneras; por ejemplo, por finalidad, propietario o entorno. Esto ayuda a encontrar rápidamente un host dedicado específico en función de las etiquetas personalizadas que asignó. Las etiquetas del host dedicado también se pueden utilizar para el seguimiento de la asignación de costos.

También puede aplicar etiquetas a hosts dedicados en el momento de su creación. Para obtener más información, consulte Asignar hosts dedicados.

Puede etiquetar un host dedicado usando los métodos siguientes.

Console

Para etiquetar un host dedicado

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Hosts dedicados (Hosts dedicados).
3. Seleccione el host dedicado que desea etiquetar y, a continuación, elija Actions (Acciones), Manage tags (Administrar etiquetas).
4. En la pantalla Manage tags (Administrar etiquetas), elija Add tag (Agregar etiqueta) y, a continuación, especifique la clave y el valor de la etiqueta.
5. (Opcional) Elija Add tag (Agregar etiqueta) para agregar etiquetas adicionales al host dedicado.
6. Elija Save changes.

AWS CLI

Para etiquetar un host dedicado

Utilice el comando create-tags de la AWS CLI.

El siguiente comando etiqueta el host dedicado especificado con `Owner=TeamA`.

```
aws ec2 create-tags --resources h-abc12345678909876 --tags Key=Owner,Value=TeamA
```

PowerShell

Para etiquetar un host dedicado

Utilice el comando New-EC2Tag de AWS Tools for Windows PowerShell.

El comando `New-EC2Tag` necesita un objeto `Tag`, que especifica el par de clave y valor que se va a utilizar para la etiqueta de host dedicado. El siguiente comando crea un objeto `Tag` denominado `$tag` con un par de clave y valor de `Owner` y `TeamA` respectivamente:

```
PS C:\> $tag = New-Object Amazon.EC2.Model.Tag
PS C:\> $tag.Key = "Owner"
PS C:\> $tag.Value = "TeamA"
```

El siguiente comando etiqueta el host dedicado especificado con el objeto `$tag`:

```
PS C:\> New-EC2Tag -Resource h-abc12345678909876 -Tag $tag
```

Monitorear hosts dedicados

Amazon EC2 monitoriza constantemente el estado de sus hosts dedicados. Las actualizaciones se comunican en la consola de Amazon EC2. Puede ver información acerca de un host dedicado utilizando los métodos siguientes.

Console

Para ver el estado de un host dedicado

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Hosts dedicados (Hosts dedicados).
3. Localice el host dedicado en la lista y revise el valor en la columna State (Estado).

AWS CLI

Para ver el estado de un host dedicado

Utilice el comando de la AWS CLI describe-hosts y, a continuación, revise la propiedad `state` en el elemento de respuesta `hostSet`.

```
aws ec2 describe-hosts --host-id h-012a3456b7890cdef
```

PowerShell

Para ver el estado de un host dedicado

Utilice el comando de AWS Tools for Windows PowerShell Get-EC2Host y, a continuación, revise la propiedad `state` en el elemento de respuesta `hostSet`.

```
PS C:\> Get-EC2Host -HostId h-012a3456b7890cdef
```

En la siguiente tabla se explican los posibles estados de host dedicado.

Estado	Descripción
`available`	AWS no ha detectado ningún problema con el host dedicado. No hay programada ninguna tarea de mantenimiento ni de reparación. Se pueden iniciar instancias en este host dedicado.
`released`	Se ha liberado el host dedicado. El ID de host ya no está en uso. Los hosts liberados no se pueden volver a usar.
`under-assessment`	AWS está estudiando un posible problema con el host dedicado. Si se debe realizar alguna acción, recibirá una notificación a través de la AWS Management Console o de un correo electrónico. Con este estado, no se pueden iniciar instancias en un host dedicado.
`pending`	El host dedicado no se puede utilizar para iniciar instancias nuevas. O bien está en proceso de modificación para admitir varios tipos de instancia o de recuperación del host.
`permanent-failure`	Se ha detectado un error no recuperable. Recibirá un aviso de expulsión a través de las instancias y por correo electrónico. Es posible que las instancias sigan funcionando. Si detiene o termina todas las instancias en un host dedicado con este estado, AWS retira el host. AWS no reinicia las instancias en este estado. Con este estado, no se pueden iniciar instancias en hosts dedicados.

Estado	Descripción
`released-permanent-failure`	AWS continuamente inicia hosts dedicados que han presentado un error y que ya no tienen instancias de ejecución en ellos. El ID de host dedicado ya no está disponible para su uso.

Liberar hosts dedicados

Es necesario detener cualquier instancia en ejecución en el host dedicado antes de poder liberarlo. Estas instancias se pueden migrar a otros hosts dedicados en la cuenta de forma que pueda seguir usándolas. Estos pasos solo se aplican a hosts dedicados bajo demanda.

Puede liberar un host dedicado usando los métodos siguientes.

Console

Para publicar un host dedicado

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Hosts dedicados (Hosts dedicados).
3. En la página Dedicated Hosts (Hosts dedicados), seleccione el host dedicado que liberar.
4. Elija Actions (Acciones), Release Hosts (Liberar hosts).
5. Para confirmar, elija Release (Liberar).

AWS CLI

Para publicar un host dedicado

Utilice el comando de la AWS CLI release-hosts.

```
aws ec2 release-hosts --host-ids h-012a3456b7890cdef
```

PowerShell

Para publicar un host dedicado

Utilice el comando de AWS Tools for Windows PowerShell Remove-EC2Hosts.

```
PS C:\> Remove-EC2Hosts -HostId h-012a3456b7890cdef
```

Después de liberar un host dedicado, no puede volver a utilizar el mismo host o ID de host y ya no se le cobrarán tarifas de facturación bajo demanda del host. El estado del host dedicado se cambia a `released` y ya no puede iniciar ninguna instancia en ese host.

> **Note**
>
> Si ha publicado recientemente hosts dedicados, puede pasar algún tiempo hasta que dejen de contabilizarse para su límite. Durante este tiempo, puede experimentar errores de `LimitExceeded` al intentar asignar nuevos hosts dedicados. Si este es el caso, intente volver a asignar nuevos hosts pasados unos minutos.

Las instancias que se detuvieron aún están disponibles para su uso y aparecen listadas en la página Instances (instancia[s]). Las instancias conservan su configuración de tenencia `host`.

Adquirir un Reservas de hosts dedicados

Puede comprar reservas utilizando los siguientes métodos:

Console

Para comprar reservas

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. Elija Dedicated Hosts (Hosts dedicados), Dedicated Host Reservations (Reservas de hosts dedicados), Purchase Dedicated Host Reservation (Comprar Reserva de host dedicado).
3. En la pantalla Buscar ofertas, haga lo siguiente:
   a. En Familia de instancias, seleccione la familia de instancias del host dedicado para la que quiera comprar la reserva de host dedicado.
   b. En Opción de pago, seleccione y configure la opción de pago que prefiera.
4. Elija Siguiente.
5. Seleccione los hosts dedicados a los que quiera asociar la reserva de host dedicado y, a continuación, seleccione Siguiente.
6. (Opcional) Asigne etiquetas a la reserva de host dedicado.
7. Revise su pedido y elija Comprar.

AWS CLI

Para comprar reservas

1. Utilice el comando de la AWS CLI describe-host-reservation-offerings para mostrar las ofertas disponibles que se ajustan a sus necesidades. En los ejemplos siguientes se muestran las ofertas que admiten instancias en la familia de instancias `m4` y tienen un plazo de un año.

   > **Note**
   >
   > Las condiciones de la oferta se especifican en segundos. Unas condiciones de la oferta de un año incluyen 31 536 000 segundos y unas condiciones de la oferta de tres años incluyen 94 608 000 segundos.

   ```
   aws ec2 describe-host-reservation-offerings --filter Name=instance-
   family,Values=m4 --max-duration 31536000
   ```

   El comando devuelve una lista de ofertas que coinciden con sus criterios. Tenga en cuenta el `offeringId` de la oferta que comprar.

2. Utilice el comando de la AWS CLI purchase-host-reservation para comprar la oferta y proporcionar el `offeringId` indicado en el paso anterior. En el siguiente ejemplo se compra la reserva especificada y se asocia a un host dedicado específico que ya está asignado en la cuenta de AWS, y se aplica una etiqueta con una clave de `purpose` y un valor de `production`.

   ```
   aws ec2 purchase-host-reservation --offering-id hro-03f707bf363b6b324 --
   host-id-set h-013abcd2a00cbd123 --tag-specifications 'ResourceType=host-
   reservation,Tags={Key=purpose,Value=production}'
   ```

PowerShell

Para comprar reservas

1. Utilice el comando de AWS Tools for Windows PowerShell Get-EC2HostReservationOffering para mostrar las ofertas disponibles que se ajustan a sus necesidades. Los ejemplos

siguientes muestran las ofertas que admiten instancias en la familia de instancias `m4` y tienen unas condiciones de la oferta de un año.

> **Note**
>
> Las condiciones de la oferta se especifican en segundos. Unas condiciones de la oferta de un año incluyen 31 536 000 segundos y unas condiciones de la oferta de tres años incluyen 94 608 000 segundos.

```
PS C:\> $filter = @{Name="instance-family"; Value="m4"}
```

```
PS C:\> Get-EC2HostReservationOffering -filter $filter -MaxDuration 31536000
```

El comando devuelve una lista de ofertas que coinciden con sus criterios. Tenga en cuenta el `offeringId` de la oferta que comprar.

2. Utilice el comando de AWS Tools for Windows PowerShell New-EC2HostReservation para comprar la oferta y proporcionar el `offeringId` indicado en el paso anterior. En el siguiente ejemplo se compra la reserva especificada y se asocia a un host dedicado específico que ya está asignado en la cuenta de AWS.

```
PS C:\> New-EC2HostReservation -OfferingId hro-03f707bf363b6b324 -
HostIdSet h-013abcd2a00cbd123
```

Ver reservas del host dedicado

Puede ver información acerca de los hosts dedicados asociados con su reserva, incluido lo siguiente:

- El plazo de la reserva
- La opción de pago
- Las fechas de inicio y finalización de la reserva

Puede ver los detalles de sus reservas de host dedicado utilizando los siguientes métodos.

Console

Para ver los detalles de una reserva de host dedicado

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Hosts dedicados.
3. En la página Dedicated Hosts (Hosts dedicados), elija Dedicated Host Reservations (Reservas de hosts dedicados) y, a continuación, seleccione la reserva de la lista proporcionada.
4. Elija Details (Detalles) para obtener información acerca de la reserva.
5. Elija Hosts para obtener información acerca de los hosts dedicados con los que está asociada la reserva.

AWS CLI

Para ver los detalles de una reserva de host dedicado

Utilice el comando de la AWS CLI describe-host-reservations.

```
aws ec2 describe-host-reservations
```

PowerShell

Para ver los detalles de una reserva de host dedicado

Utilice el comando de AWS Tools for Windows PowerShell Get-EC2HostReservation.

```
PS C:\> Get-EC2HostReservation
```

Asignar etiquetas al Reservas de hosts dedicados

Puede asignar etiquetas personalizadas a sus Reservas de hosts dedicados para clasificarlos de diversas maneras; por ejemplo, por finalidad, propietario o entorno. Esto ayuda a encontrar rápidamente un Reserva de host dedicado específico en función de las etiquetas personalizadas que asignó.

Solo puede etiquetar un Reserva de host dedicado mediante las herramientas de la línea de comandos.

AWS CLI

Para etiquetar un Reserva de host dedicado

Utilice el comando create-tags de la AWS CLI.

```
aws ec2 create-tags --resources hr-1234563a4ffc669ae --tags Key=Owner,Value=TeamA
```

PowerShell

Para etiquetar un Reserva de host dedicado

Utilice el comando New-EC2Tag de AWS Tools for Windows PowerShell.

El comando `New-EC2Tag` necesita un parámetro `Tag`, que especifica el par de clave y valor que se va a utilizar para la etiqueta de Reserva de host dedicado. Los siguientes comandos crean el parámetro `Tag`.

```
PS C:\> $tag = New-Object Amazon.EC2.Model.Tag
PS C:\> $tag.Key = "Owner"
PS C:\> $tag.Value = "TeamA"
```

```
PS C:\> New-EC2Tag -Resource hr-1234563a4ffc669ae -Tag $tag
```

Utilizar hosts dedicados compartidos

El uso compartido de un host dedicado permite a los propietarios de un host dedicado compartir su host dedicado con otras cuentas de AWS o dentro de una organización de AWS. Esto permite crear y administrar los hosts dedicados de forma centralizada y compartir el host dedicado entre varias cuentas de AWS o dentro de su organización de AWS.

En este modelo, la cuenta de AWS que posee el host dedicado (propietario) lo comparte con otras cuentas de AWS (consumidores). Los consumidores pueden iniciar instancias en hosts dedicados que comparten con ellos de la misma forma que harían con los hosts dedicados que poseen en su propia cuenta. El propietario es responsable de administrar el host dedicado y las instancias que inician en él. Los propietarios no pueden modificar las instancias que los consumidores inician en hosts dedicados compartidos. Los consumidores son responsables de administrar las instancias que inician en hosts dedicados compartidos con ellos. Los consumidores no pueden ver ni modificar instancias propiedad de otros consumidores o del propietario de host dedicado, y no pueden modificar los hosts dedicados que se comparten con ellos.

Un propietario de un host dedicado puede compartir un host dedicado con:

- Cuentas específicas de AWS dentro o fuera de su organización de AWS
- Una unidad organizativa dentro de su organización de AWS
- Toda su organización de AWS

Contenido

Requisitos previos para compartir hosts dedicados

- Para compartir un host dedicado, debe ser el propietario en su cuenta de AWS. No puede compartir un host dedicado que se ha compartido con usted.
- Para compartir un host dedicado con su organización de AWS o una unidad organizativa de AWS, debe habilitar el uso compartido con AWS Organizations. Para obtener más información, consulte Habilitar el uso compartido con AWS Organizations en la Guía del usuario de AWS RAM.

Limitaciones para compartir host dedicado

No puede compartir hosts dedicados que se hayan asignado para los siguientes tipos de instancia: `u-6tb1.metal`, `u-9tb1.metal`, `u-12tb1.metal`, `u-18tb1.metal` y `u-24tb1.metal`.

Servicios relacionados

AWS Resource Access Manager

El uso compartido de un host dedicado se integra con AWS Resource Access Manager (AWS RAM). AWS RAM es un servicio que le permite compartir sus recursos de AWS con cualquier cuenta de AWS o a través de AWS Organizations. Con AWS RAM, puede compartir recursos de su propiedad creando un uso compartido de recursos. Un uso compartido de recursos especifica los recursos que compartir y los consumidores con quienes compartirlos. Los consumidores pueden ser cuentas de AWS individuales, unidades organizativas o toda una organización de AWS Organizations.

Para obtener más información sobre AWS RAM, consulte la Guía del usuario de AWS RAM.

Compartir el uso entre zonas de disponibilidad

Para garantizar que los recursos se distribuyen por todas las zonas de disponibilidad de una región, asignamos zonas de disponibilidad de manera independiente a nombres de cada cuenta. Esto podría dar lugar a diferencias de nomenclatura de zona de disponibilidad entre cuentas. Por ejemplo, es posible que la zona de disponibilidad `us-east-1a` de su cuenta de AWS no se encuentre en la misma ubicación de `us-east-1a` que otra cuenta de AWS.

Para identificar la ubicación de los hosts dedicados relativa a las cuentas, debe utilizar el ID de zona de disponibilidad (ID de AZ). El ID de zona de disponibilidad es un identificador único e idéntico para una zona de disponibilidad en todas las cuentas de AWS. Por ejemplo, `use1-az1` es un ID de zona de disponibilidad para la región `us-east-1` y está en la misma ubicación en todas las cuentas de AWS.

Para ver los ID de zona de disponibilidad de las zonas de disponibilidad de su cuenta

1. Abra la consola de AWS RAM en https://console.aws.amazon.com/ram.
2. Los ID de zona de disponibilidad de la región actual se muestran en el panel Your AZ ID (Su ID de AZ) en el lado derecho de la pantalla.

Compartir un host dedicado

Cuando un propietario comparte un host dedicado, permite a los consumidores iniciar instancias en el host. Los consumidores pueden iniciar tantas instancias en el host compartido como lo permita su capacidad disponible.

> **Important**
>
> Tenga en cuenta que es responsable de asegurarse de que tiene los derechos de licencia adecuados para compartir cualquier licencia BYOL en sus hosts dedicados.

Si comparte un host dedicado con la ubicación automática habilitada, tenga en cuenta lo siguiente, ya que podría provocar que el host dedicado se usara de una forma no deseada:

- Si los consumidores inician instancias con la tenencia de host dedicado y no tienen capacidad en un host dedicado que poseen en su cuenta, la instancia se inicia automáticamente en el host dedicado compartido.

Para compartir un host dedicado, debe añadirlo al recurso compartido. Un uso compartido de recursos es un recurso de AWS RAM que le permite compartir los recursos a través de cuentas de AWS. Un uso compartido de recursos especifica los recursos que compartir y los consumidores con quienes se comparten. Puede añadir el host dedicado a un recurso existente o puede añadirlo a un nuevo recurso compartido.

Si forma parte de una organización en AWS Organizations y está habilitado el uso compartido en la organización, los consumidores de su organización obtienen acceso automáticamente al host dedicado compartido. De lo contrario, los consumidores reciben una invitación para unirse al recurso compartido y se les concede acceso al host dedicado compartido después de aceptar la invitación.

> **Note**
>
> Después de compartir un host dedicado, los consumidores podrían tardar unos minutos en tener acceso a ella.

Puede compartir host dedicado que tenga mediante uno de los métodos siguientes.

Amazon EC2 console

Para compartir un host dedicado que posee utilizando la consola de Amazon EC2, realice el siguiente procedimiento:

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

2. En el panel de navegación, seleccione Hosts dedicados (Hosts dedicados).
3. Elija host dedicado para compartir y seleccione Acciones, Compartir reserva.
4. Seleccione el uso compartido al que añadir host dedicado y elija Compartir host.

   Los consumidores pueden tardar algunos minutos en obtener acceso al host compartido.

AWS RAM console

Compartir un host dedicado que posee utilizando la consola de AWS RAM

Consulte Crear un recurso compartido en la Guía del usuario de AWS RAM.

AWS CLI

Compartir un host dedicado que posee mediante AWS CLI

Utilice el comando create-resource-share.

Anular un host dedicado compartido

El propietario del host dedicado puede dejar de compartir un host dedicado compartido en cualquier momento. Cuando se deja de compartir un host dedicado compartido, se aplican las reglas siguientes:

- Los consumidores con los que se compartió el host dedicado ya no pueden iniciar nuevas instancias en él.
- Las instancias propiedad de los consumidores que se estaban ejecutando en el host dedicado en el momento de dejar de compartir continúan ejecutándose, pero se programan para su retirada. Los consumidores reciben notificaciones de retirada para las instancias y tienen dos semanas para actuar a raíz de estas notificaciones. Sin embargo, si el host dedicado se vuelve a compartir con el consumidor dentro del período de notificación de retirada, la retirada de la instancia se cancela.

Para dejar de compartir un host dedicado compartido que posee, debe quitarlo del recurso compartido. Para ello, puede realizar uno de los siguientes métodos.

Amazon EC2 console

Para dejar de compartir un host dedicado compartido que posee utilizando la consola de Amazon EC2, realice el siguiente procedimiento:

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Hosts dedicados (Hosts dedicados).
3. Elija la host dedicado que desea dejar de compartir y elija la pestaña Uso compartido.
4. La pestaña Uso compartido muestra los usos compartidos de recursos a los que se ha añadido la host dedicado. Seleccione el uso compartido de recurso desde el que desea quitar la host dedicado y elija Quitar host de recurso compartido.

AWS RAM console

Dejar de compartir un host dedicado compartido que posee utilizando la consola de AWS RAM

Consulte Actualizar un recurso compartido en la Guía del usuario de AWS RAM.

Command line

Dejar de compartir un host dedicado compartido que posee mediante la consola de AWS CLI

Utilice el comando disassociate-resource-share.

Identificar un host dedicado compartido

Los propietarios y consumidores pueden identificar hosts dedicados compartidos mediante uno de los siguientes métodos.

Amazon EC2 console

Para identificar un host dedicado compartido utilizando la consola de Amazon EC2

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Hosts dedicados (Hosts dedicados). La pantalla muestra los hosts dedicados que posee y los hosts dedicados que se comparten con usted. La columna Owner (Propietario) muestra el ID de la cuenta de AWS del propietario del host dedicado.

Command line

Identificar un host dedicado compartido mediante AWS CLI

Utilice el comando describe-hosts. El comando devuelve los hosts dedicados que posee y los hosts dedicados que se comparten con usted.

Ver instancias que se ejecutan en un host dedicado compartido

Los propietarios y consumidores pueden ver las instancias que se ejecutan en un host dedicado compartido en cualquier momento mediante uno de los métodos siguientes.

Amazon EC2 console

Para ver las instancias que se ejecutan en un host dedicado compartido mediante la consola de Amazon EC2

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Hosts dedicados (Hosts dedicados).
3. Seleccione el host dedicado para el que desea ver las instancias y elija Instances (instancia[s]). La pestaña muestra las instancias que se ejecutan en el host. Los propietarios ven todas las instancias que se ejecutan en el host, incluidas las instancias iniciadas por los consumidores. Los consumidores solo ven las instancias en ejecución que iniciaron en el host. La columna Owner (Propietario) muestra el ID de cuenta de AWS de la cuenta que lanzó la instancia.

Command line

Ver las instancias que se ejecutan en un host dedicado compartido mediante AWS CLI

Utilice el comando describe-hosts. El comando devuelve las instancias que se ejecutan en cada host dedicado. Los propietarios ven todas las instancias que se ejecutan en el host. Los consumidores solo ven las instancias en ejecución que iniciaron en los hosts compartidos. `InstanceOwnerId` muestra el ID de cuenta de AWS del propietario de la instancia.

Permisos de host dedicado compartido

Permisos de los propietarios

Los propietarios son responsables de administrar sus hosts dedicados compartidos y las instancias que inician en ellos. Los propietarios pueden ver todas las instancias que se ejecutan en el host dedicado compartido, incluidas las iniciadas por los consumidores. Sin embargo, los propietarios no pueden realizar ninguna acción en las instancias en ejecución iniciadas por los consumidores.

Permisos de los consumidores

Los consumidores son responsables de administrar las instancias que inician en un host dedicado compartido. Los consumidores no pueden modificar el host dedicado compartido en modo alguno y no pueden ver ni modificar las instancias que iniciaron otros consumidores o el propietario del host dedicado.

Facturación y medición

No se aplican cargos adicionales por compartir hosts dedicados.

A los propietarios se les cobran los hosts dedicados que comparten. A los consumidores no se les cobran las instancias que inician en hosts dedicados compartidos.

Las Reservas de hosts dedicados continúan proporcionando descuentos de facturación para los hosts dedicados compartidos. Solo los propietarios de host dedicado pueden comprar Reservas de hosts dedicados para los hosts dedicados compartidos que poseen.

Límites de host dedicado

Los hosts dedicados compartidos se contabilizan solo para los límites de hosts dedicados del propietario. Los límites de hosts dedicados del consumidor no se ven afectados por los hosts dedicados que se hayan compartido con ellos. Del mismo modo, las instancias que los consumidores inician en hosts dedicados compartidos no se contabilizan para sus límites de instancia.

Recuperación de host y uso compartido de host dedicado

La recuperación del host recupera instancias iniciadas por el propietario del host dedicado y los consumidores con los que se ha compartido. El host dedicado de sustitución se asigna a la cuenta del propietario. Se añade a los mismos recursos compartidos que el host dedicado original y se comparte con los mismos consumidores.

Para obtener más información, consulte Recuperación de host.

Hosts dedicados en AWS Outposts

AWS Outposts es un servicio completamente administrado que extiende la infraestructura, los servicios, las API y las herramientas de AWS a sus instalaciones. Cuando se brinda acceso local a la infraestructura administrada de AWS, AWS Outposts le permite crear y ejecutar aplicaciones en las instalaciones mediante el uso de las mismas interfaces de programación que en las regiones de AWS, al mismo tiempo que utiliza recursos de computación y de almacenamiento locales para reducir la latencia y las necesidades de procesamiento de datos locales.

Un Outpost es un grupo de capacidad informática y de almacenamiento de AWS implementada en un sitio del cliente. AWS opera, supervisa y administra esta capacidad como parte de una región de AWS.

Puede asignar hosts dedicados en Outposts que tiene en su cuenta. Esto le facilita traer a AWS Outposts sus licencias de software y cargas de trabajo existentes que requieren un servidor físico dedicado. También puede asignar activos de hardware específicos a un Outpost para ayudar a minimizar la latencia entre las cargas de trabajo.

Los hosts dedicados le permiten utilizar las licencias de software elegibles en Amazon EC2, para que obtenga la flexibilidad y la rentabilidad del uso de sus propias licencias. Otras licencias de software que están vinculadas a máquinas virtuales, sockets o núcleos físicos también se pueden utilizar en hosts dedicados, sujeto a los términos de licencia. Aunque los Outposts siempre han sido entornos de inquilino único que son elegibles para cargas de trabajo BYOL, los hosts dedicados permiten limitar las licencias necesarias a un solo host en lugar de toda la implementación de Outpost.

Además, el uso de hosts dedicados en un Outpost brinda mayor flexibilidad en la implementación del tipo de instancia y un control más minucioso sobre la ubicación de la instancia. Puede apuntar a un host específico para los inicializacións de las instancias y utilizar la afinidad de host para asegurarse de que la instancia siempre se ejecute en ese host, o puede utilizar la ubicación automática para iniciar una instancia en cualquier host disponible que tenga configuraciones coincidentes y capacidad disponible.

Contenido

- Asignación y uso de un host dedicado en un Outpost

Requisitos previos

Debe tener un Outpost instalado en su sitio. Para obtener más información, consulte Crear una instancia de Outpost y solicitar capacidad de Outpost en la Guía del usuario de AWS Outposts.

Características admitidas

- Se admiten las siguientes familias de instancias: `C5`, `M5`, `R5`, `C5d`, `M5d`, `R5d`, `G4dn` e `i3en`.
- Los hosts dedicados en Outposts se pueden configurar para que admitan varios tamaños de instancias. La compatibilidad con varios tamaños de instancia está disponible para las siguientes familias de instancias: `C5`, `M5`, `R5`, `C5d`, `M5d` y `R5d`. Para obtener más información, consulte Configuraciones de capacidad de instancias.
- Los hosts dedicados en Outposts admiten la ubicación automática y los inicializacións de instancias con destino. Para obtener más información, consulte Comprender la colocación automática y afinidad.
- Los hosts dedicados en Outposts admiten la afinidad de host. Para obtener más información, consulte Comprender la colocación automática y afinidad.
- Los hosts dedicados en Outposts admiten el uso compartido con AWS RAM. Para obtener más información, consulte Utilizar hosts dedicados compartidos.

Consideraciones

- Las reservas de host dedicado no se admiten en Outposts.
- Los grupos de recursos de host y AWS License Manager no se admiten en Outposts.
- Los hosts dedicados en Outposts no admiten instancias T3 ampliables.
- Los hosts dedicados en Outposts no admiten la recuperación de host.
- Las instancias con tenencia de hosts dedicados en Outposts no son compatibles con la recuperación automática simplificada.

Asignación y uso de un host dedicado en un Outpost

Usted asigna y utiliza hosts dedicados en Outposts de la misma manera que haría con los hosts dedicados en una región de AWS.

Requisitos previos

Cree una subred en el Outpost. Para obtener más información, consulte Crear una subred en la Guía del usuario de AWS Outposts.

Para asignar un host dedicado en un Outpost, utilice uno de los métodos a continuación:

AWS Outposts console

1. Abra la consola de AWS Outposts en https://console.aws.amazon.com/outposts/.
2. En el panel de navegación, elija Outposts. Seleccione el Outpost y luego, elija Actions (Acciones), Allocate Dedicated Host (Asignar un host dedicado).
3. Configure el host dedicado según sea necesario. Para obtener más información, consulte Asignar hosts dedicados.

   > **Note**
   >
   > Los campos Availability Zone (Zona de disponibilidad) y Outpost ARN (ARN de Outpost) deben rellenarse previamente con la zona de disponibilidad y el ARN del Outpost seleccionado.

4. Elija Asignar.

Amazon EC2 console

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Dedicated Hosts (Hosts dedicados) y, a continuación, elija Allocate Dedicated Host (Asignar host dedicado).
3. En Availability Zone (Zona de disponibilidad), seleccione la zona de disponibilidad asociada al Outpost.
4. En Outpost ARN (ARN de Outpost), ingrese el ARN del Outpost.
5. Para dirigirse a activos de hardware específicos en Outpost, en Dirigirse a activos de hardware específicos en Outpost, seleccione Habilitar. Para cada activo de hardware al que se dirija, elija Agregar ID de activo y, a continuación, ingrese el ID de activo de hardware.

> **Note**
>
> El valor que especifique para Cantidad debe ser igual al número de ID de activos que especifique. Por ejemplo, si especificas 3 ID de activos, la cantidad también debe ser 3.

6. Configure el host dedicado restante según sea necesario. Para obtener más información, consulte Asignar hosts dedicados.
7. Elija Asignar.

AWS CLI

Utilice el comando de la AWS CLI allocate-hosts. En `--availability-zone`, especifique la zona de disponibilidad asociada al Outpost. En `--outpost-arn`, especifique el ARN del Outpost. Si lo desea, en `--asset-ids`, especifique los ID de los activos de hardware de Outpost a los que se dirigirá.

```
aws ec2 allocate-hosts --availability-zone "us-east-1a" --outpost-arn
 "arn:aws:outposts:us-east-1a:111122223333:outpost/op-4fe3dc21baEXAMPLE" --asset-
ids asset_id --instance-family "m5" --auto-placement "off" --quantity 1
```

Para iniciar una instancia en un host dedicado en un Outpost

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Hosts dedicados (Hosts dedicados). Seleccione el host dedicado que asignó en el paso anterior y elija Actions (Acciones), Launch instance onto host (iniciar instancia en el host).
3. Configure la instancia según sea necesario y luego lance la instancia. Para obtener más información, consulte iniciar instancias en un host dedicado.

Recuperación de host

La recuperación del host dedicado reinicia las instancias en un nuevo host de sustitución cuando se detectan ciertas condiciones problemáticas en el host dedicado. La recuperación del host reduce la necesidad de intervención manual y reduce la carga operativa si se produce un error de host

dedicado inesperado que involucre a la alimentación del sistema o a eventos de conectividad de red. Para recuperarse de otros problemas de host dedicado se requerirá de una intervención manual.

Contenido

Conceptos básicos de la recuperación del host

Los hosts dedicados y el proceso de recuperación de grupos de recursos de host utilizan comprobaciones de estado a nivel de host para acceder a la disponibilidad de host dedicado y para detectar errores subyacentes del sistema. El tipo de error de host dedicado determina si es posible la recuperación automática del host dedicado. Entre los ejemplos de problemas que provocan errores en las comprobaciones de estado en el nivel de host se incluyen:

- Pérdida de conectividad de red
- Pérdida de potencia del sistema
- Problemas de hardware o software en el host físico

> **Important**
>
> La recuperación automática de los hosts dedicados no se produce cuando el host está programado para retirarse.

Recuperación automática de host dedicado

Cuando se detecta un error de alimentación del sistema o de conectividad de red en el host dedicado, se inicia la recuperación automática del host y Amazon EC2 asigna automáticamente un host dedicado de sustitución en la misma zona de disponibilidad que el host dedicado original. El

host dedicado de sustitución recibe un nuevo ID de host, pero conserva los mismos atributos que el host dedicado original, incluidos:

- Zona de disponibilidad
- Tipo de instancia
- Etiquetas
- Configuración de colocación automática
- Reserva

Tras asignar el host dedicado de sustitución, se recuperan las instancias en este. Las instancias recuperadas conservan los mismos atributos que las instancias originales, incluidos:

- ID de instancia
- Direcciones IP privadas
- Direcciones IP elásticas
- Asociaciones de volumen de EBS
- Todos los metadatos de la instancia

Además, la integración incorporada con AWS License Manager automatiza el seguimiento y la administración de las licencias si se produce una recuperación del host.

> **Note**
>
> Solo se admite integración con AWS License Manager en las regiones en las que AWS License Manager está disponible.

Si las instancias tienen una relación de afinidad de host con el host dedicado deteriorado, las instancias recuperadas establecen la afinidad de host con el host dedicado de sustitución.

Cuando se han recuperado todas las instancias en el host dedicado de sustitución, se libera el host dedicado deteriorado y el host dedicado de sustitución empieza a estar disponible para su uso.

Cuando se inicia la recuperación del host, el propietario de la cuenta de AWS recibe una notificación por correo electrónico y a través de un evento de AWS Health Dashboard. Después de que la recuperación del host se haya completado correctamente, se envía una segunda notificación.

Si usa License Manager de AWS para realizar un seguimiento de sus licencias, License Manager de AWS asigna nuevas licencias al host dedicado de sustitución en función de los límites de configuración de la licencia. Si la configuración de la licencia tiene límites invariables que se traspasarían como resultado de la recuperación del host, no se permite el proceso de recuperación y recibirá un aviso de error en la recuperación del host en forma de notificación de Amazon SNS (siempre que se hayan configurado las notificaciones para AWS License Manager). Si la configuración de la licencia tiene límites flexibles que se traspasarían como resultado de la recuperación del host, no se permite continuar con la recuperación y recibirá un aviso del traspaso del límite en forma de notificación de Amazon SNS. Para obtener más información, consulte Uso de configuraciones de licencia y Configuraciones en License Manager en la Guía del usuario de AWS License Manager.

Escenarios sin recuperación automática de host dedicado

La recuperación automática de los hosts dedicados no se produce cuando el host está programado para retirarse. Recibirá una notificación de retiro en el AWS Health Dashboard, un evento de Amazon CloudWatch y en la dirección de email del propietario de la cuenta de AWS recibirá un mensaje sobre el error del host dedicado. Siga los pasos de corrección descritos en la notificación de retirada dentro del plazo de tiempo indicado para recuperar manualmente las instancias en el host que se va a retirar.

Las instancias detenidas no se recuperan en el host dedicado de sustitución. Si intenta iniciar una instancia detenida en el host dedicado deteriorado, el inicio de la instancia produce un error. Recomendamos que modifique la instancia detenida para que se dirija a un host dedicado diferente o que la lance en un host dedicado disponible con configuraciones coincidentes y colocación automática habilitada.

Las instancias con almacenamiento de la instancia no se recuperan en el host dedicado de sustitución. Como solución, se señala el host dedicado deteriorado para que se retire y usted recibe una notificación de retirada después de que se haya completado la recuperación del host. Siga los pasos de corrección descritos en la notificación de retirada dentro del plazo de tiempo indicado para recuperar manualmente las instancias restantes en el host dedicado deteriorado.

Tipos de instancias admitidas

La recuperación de host es compatible con las siguientes familias de instancias: A1, C3, C4, C5, C5n, C6a, C6g, C6i, Inf1, G3, G5g, M3, M4, M5, M5n, M5zn, M6a, M6g, M6i, P2, P3, R3, R4, R5, R5b, R5n, R6g, R6i, T3, X1, X1e, X2iezn, u-6tb1, u-9tb1, u-12tb1, u-18tb1 y u-24tb1.

Para recuperar instancias no compatibles, vea Recuperar de forma manual instancias no admitidas.

> **Note**
>
> La recuperación automática de host dedicado en los tipos de instancia de metal compatible tomará más tiempo en detectarse y recuperarse que en los tipos de instancia no metálicas.

Configurar la recuperación del host

Puede configurar la recuperación del host en el momento de la asignación del host dedicado o después de la asignación mediante la consola de Amazon EC2 o la AWS Command Line Interface (CLI).

Contenido

Habilitar la recuperación del host

Puede habilitar la recuperación del host en el momento de la asignación del host dedicado o después de la asignación.

Para obtener más información sobre la habilitación de la recuperación del host en el momento de la asignación del host dedicado, consulte Asignar hosts dedicados.

Para habilitar la recuperación del host después de la asignación con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Hosts dedicados (Hosts dedicados).
3. Seleccione el host dedicado para el que desea habilitar la recuperación del host y elija Actions (Acciones), Modify Host Recovery (Modificar recuperación del host).
4. En Host recovery (Recuperación del host), elija Enable (Habilitar) y, a continuación, elija Save (Guardar).

Para habilitar la recuperación del host después de la asignación con la AWS CLI

Utilice el comando modify-hosts y especifique el parámetro `host-recovery`.

```
$ aws ec2 modify-hosts --host-recovery on --host-ids h-012a3456b7890cdef
```

Deshabilitar la recuperación del host

Puede deshabilitar la recuperación del host en cualquier momento después de la asignación del host dedicado.

Para deshabilitar la recuperación del host después de la asignación (consola)

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Hosts dedicados (Hosts dedicados).
3. Seleccione el host dedicado para el que desea deshabilitar la recuperación del host y elija Actions (Acciones), Modify Host Recovery (Modificar recuperación del host).
4. En Host recovery (Recuperación del host), elija Disable (Deshabilitar) y, a continuación, elija Save (Guardar).

Para deshabilitar la recuperación del host después de la asignación con AWS CLI

Utilice el comando modify-hosts y especifique el parámetro `host-recovery`.

```
$ aws ec2 modify-hosts --host-recovery off --host-ids h-012a3456b7890cdef
```

Ver la configuración de la recuperación del host

Puede ver la configuración de la recuperación del host de un host dedicado en cualquier momento.

Para ver la configuración de la recuperación del host de un host dedicado con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Hosts dedicados (Hosts dedicados).
3. Seleccione el host dedicado y en la pestaña Description (Descripción), revise el campo Host Recovery (Recuperación del host).

Ver la configuración de la recuperación del host de un host dedicado mediante AWS CLI

Utilice el comando describe-hosts.

```
$ aws ec2 describe-hosts --host-ids h-012a3456b7890cdef
```

El elemento de respuesta `HostRecovery` indica si la recuperación del host está habilitada o deshabilitada.

Estados de recuperación del host

Cuando se detecta un error del host dedicado, el host dedicado afectado adopta el estado `under-assessment` y todas las instancias pasan al estado `impaired`. No puede iniciar instancias en el host dedicado deteriorado mientras tengan el estado `under-assessment`.

Después de la asignación del host dedicado de sustitución, pasa al estado `pending`. Sigue en ese estado hasta que se complete el proceso de recuperación del host. No puede iniciar instancias en el host dedicado de sustitución mientras tengan el estado `pending`. Las instancias recuperadas en el host dedicado de sustitución siguen en el estado `impaired` durante el proceso de recuperación.

Una vez completada la recuperación del host, el host dedicado de sustitución pasa al estado `available` y las instancias recuperadas vuelven al estado `running`. Puede iniciar instancias en el host dedicado de sustitución cuenta entra en el estado `available`. El host dedicado deteriorado original se libera permanentemente y pasa al estado `released-permanent-failure`.

Si el host dedicado deteriorado tiene instancias que no admiten recuperación del host, como instancias con volúmenes respaldados por almacén de instancias, el host dedicado no se libera. En cambio, se señala para que se retire y pasa al estado `permanent-failure`.

Recuperar de forma manual instancias no admitidas

La recuperación del host no admite la recuperación de instancias que usan volúmenes de almacén de instancias. Siga las instrucciones a continuación para recuperar manualmente las instancias que no se pueden recuperar de forma automática.

> **Warning**
>
> Los datos almacenados en volúmenes del almacén de instancias se pierden cuando una instancia se detiene, se termina o se pone en hibernación. Esto incluye volúmenes de almacén de instancias adjuntadas a una instancia que tiene un volumen de EBS como dispositivo raíz. Para proteger los datos de los volúmenes de almacenamiento de instancias, realice una copia de seguridad en el almacenamiento persistente antes de que se detenga o termine la instancia.

Recuperar de forma manual instancias respaldadas por EBS

Para instancias respaldadas por EBS que no pueden recuperarse automáticamente, recomendamos que detenga e inicie las instancias manualmente para recuperarlas en un nuevo host dedicado. Para obtener más información acerca de cómo detener la instancia, así como acerca de los cambios que se producen en la configuración de la instancia cuando se detiene, consulte Detención e iniciación de una instancia de Amazon EC2.

Recuperar de forma manual instancias con respaldo en el almacén de instancias

Para instancias con respaldo en el almacén de instancias que no pueden recuperarse automáticamente, recomendamos que haga lo siguiente:

1. iniciar una instancia de sustitución en un host dedicado nuevo desde su AMI más reciente.
2. Migrar todos los datos necesarios a la instancia de sustitución.
3. Terminar la instancia original en el host dedicado deteriorado.

Servicios relacionados

host dedicado se integra con las siguientes servicios:

- AWS License Manager: realiza un seguimiento de las licencias en sus hosts dedicados de Amazon EC2 (solo se admite en regiones en las que AWS License Manager está disponible). Para obtener más información, consulte la Guía del usuario de AWS License Manager.

Precios

No hay cargos adicionales por usar la recuperación del host, pero se aplican los cargos de host dedicado habituales. Para obtener más información, consulte Precios de hosts dedicados de Amazon EC2.

Tan pronto como se inicie la recuperación del host, dejará de facturarse el host dedicado deteriorado. La facturación por el host dedicado de sustitución empieza solo cuando entra en el estado `available`.

Si el host dedicado deteriorado se facturaba usando una tarifa bajo demanda, el host dedicado de sustitución también se facturará usando una tarifa bajo demanda. Si el host dedicado deteriorado tenía una Reserva de host dedicado activa, esta se transferirá al host dedicado de sustitución.

Mantenimiento del host

Con el mantenimiento del host, las instancias de Amazon EC2 de un host dedicado degradado se reinician automáticamente en un host dedicado de reemplazo durante un evento de mantenimiento programado. Esto ayuda a reducir el tiempo de inactividad de las aplicaciones y reduce la carga pesada e indiferenciada del mantenimiento a AWS. El mantenimiento del host también se realiza para el mantenimiento planificado y rutinario de Amazon EC2.

El mantenimiento del host se admite en todas las nuevas asignaciones de hosts dedicados realizadas a través de la consola de Amazon EC2. Para cualquier host dedicado de su servidor dedicado de su Cuenta de AWS o para cualquier host dedicado nuevo asignado a través de la API AllocateHosts, puede configurar el mantenimiento del host para los hosts dedicados compatibles. Para obtener más información, consulte the section called “Configuración del mantenimiento del host”.

Contenido

Conceptos básicos del mantenimiento del host

Cuando se detecta una degradación en un host dedicado, se asigna uno nuevo. La degradación puede deberse a la degradación del hardware subyacente o a la detección de ciertas condiciones problemáticas. Las instancias del host dedicado degradado están programadas para que se reinicien automáticamente en el host dedicado de reemplazo.

El host dedicado de sustitución recibe un nuevo ID de host, pero conserva los mismos atributos que el host dedicado original. Estos atributos incluyen lo siguiente.

- Configuración de colocación automática
- Zona de disponibilidad
- Reserva
- Afinidad de hosts
- Configuración de mantenimiento del host
- Configuración de recuperación del host
- Tipo de instancia
- Etiquetas

El mantenimiento del host está disponible en todas las Regiones de AWS para los hosts dedicados compatibles. Para obtener más información acerca de los alojamientos dedicados en los que no se admite el mantenimiento del host, consulte the section called “Limitaciones”.

Su host dedicado degradado se libera después de que todas sus instancias se hayan reiniciado en un nuevo host dedicado o se hayan detenido. Puede acceder a sus instancias en el host dedicado degradado antes del evento de mantenimiento programado, pero no se admite la inicialización de instancias en el host dedicado degradado.

Puede usar el host dedicado de reemplazo para iniciar nuevas instancias en el host antes del evento de mantenimiento programado. Sin embargo, parte de la capacidad de instancias del host de reemplazo está reservada para las instancias que se deben migrar desde el host degradado. No puede iniciar nuevas instancias en esta capacidad reservada. Para obtener más información, consulte the section called “instancias en hosts dedicados”.

Limitaciones

- No se admite el mantenimiento del host en AWS Outposts, las zonas locales de AWS ni en las zonas de AWS Wavelength.
- El mantenimiento del host no se puede activar ni desactivar para los hosts que ya estén dentro de un grupo de recursos de hosts Los hosts agregados a un grupo de recursos de host retienen su configuración de mantenimiento del host. Para obtener más información, consulte Grupos de recursos de hosts.
- El mantenimiento del host solo se admite en tipos de instancias específicos. Para obtener más información, consulte the section called “Tipos de instancias admitidas”.

Mantenimiento del host en comparación con la recuperación del host

En la tabla siguiente se muestran las principales diferencias entre la recuperación del host y el mantenimiento del host.

	Recuperación de host	Mantenimiento del host
Accesibilidad	Inaccesible	Accesible
Estado	`under-assessment`	`permanent-failure`
Acción	La recuperación es inmediata	Se ha programado el mantenimiento
Flexibilidad de programación	No se puede reprogramar	Se puede reprogramar
Grupo de recursos de hosts	Compatible	No compatible

Para obtener más información sobre la recuperación de hosts, consulte Recuperación de hosts.

Tipos de instancias admitidas

El mantenimiento del host se admite en las siguientes familias de instancias:

- De uso general: `A1` | `M4` | `M5` | `M5a` | `M5n` | `M5zn` | `M6a` | `M6g` | `M6i` | `M6in` | `M7a` | `M7g` | `M7i` | `T3`
- Optimizadas para computación: `C4` | `C5` | `C5a` | `C5n` | `C6a` | `C6g` | `C6gn` | `C6i` | `C6in` | `C7g` | `C7gn` | `C7i`
- Optimizadas para memoria: `R4` | `R5` | `R5a` | `R5b` | `R5n` | `R6a` | `R6g` | `R6i` | `R6in` | `R7a` | `R7g` | `R7iz` | `u-12tb1` | `u-18tb1` | `u-24tb1` | `u-3tb1` | `u-6tb1` | `u-9tb1` | `X2iezn`
- Computación acelerada: `G3` | `G5g` | `Inf1` | `P2` | `P3`

instancias en hosts dedicados

Amazon EC2 reserva automáticamente capacidad en el host de reemplazo para las instancias que se migrarán automáticamente desde el host degradado. Amazon EC2 no reserva capacidad en el host de reemplazo para las instancias que no se pueden migrar automáticamente, como las instancias con volúmenes raíz del almacén de instancias. La capacidad reservada no se puede utilizar para iniciar nuevas instancias.

> **Note**
>
> La consola de Amazon EC2 muestra la capacidad reservada como capacidad utilizada. Puede parecer que las instancias se ejecutan tanto en el host degradado como en el host de reemplazo. Sin embargo, las instancias continuarán en ejecución solo en el host degradado hasta que se detengan o se migren a la capacidad reservada del host de reemplazo.

Si detiene manualmente una instancia en el host degradado para poder migrarla automáticamente, se libera la capacidad que estaba reservada para esa instancia en el host de reemplazo y queda disponible para su uso.

Durante el evento de mantenimiento programado, las instancias del host degradado se reinician y se migran a la capacidad reservada del host dedicado de reemplazo. Las instancias migradas retienen los mismos atributos que las del host degradado, incluidos los siguientes.

- Asociaciones de volumen de EBS de Amazon
- Direcciones IP elásticas
- ID de instancia
- Metadatos de instancia
- Dirección IP privada

Puede detener e iniciar una instancia en el host degradado en cualquier momento antes de que se inicie el evento de mantenimiento programado. Al hacer esto, la instancia se reinicia en otro host y la instancia no se someterá a un mantenimiento programado. Debe actualizar la afinidad de host de la instancia con el nuevo host en el que desea reiniciar la instancia. Si detiene todas las instancias del host degradado antes de que se inicie el evento de mantenimiento, se libera el host degradado y se cancela el evento de mantenimiento. Para obtener más información, consulte Detención e iniciación de una instancia de Amazon EC2.

> **Note**
>
> Al detener e iniciar la instancia, los datos de ningún volumen de almacén local no se retienen al detener e iniciar la instancia.

Las instancias con un volumen de almacén de instancias como dispositivo raíz finalizan después de la fecha de finalización especificada. Cualquier dato en los volúmenes de almacenes de instancias se elimina cuando las instancias terminan. Las instancias terminadas se eliminan permanentemente y no se pueden volver a iniciar. Para los casos en los que los volúmenes del almacén de instancias sean el dispositivo raíz, recomendamos iniciar las instancias de reemplazo en un host dedicado diferente utilizando la imagen de máquina de Amazon más reciente y migrar todos los datos disponibles a las instancias de reemplazo antes de la fecha de terminación especificada. Para obtener más información, consulte Acciones para la retirada de la instancia.

Las instancias que no se pueden reiniciar automáticamente se detienen después de la fecha especificada. Puede volver a iniciar estas instancias en un host diferente. Las instancias que utilizan un volumen de Amazon EBS como dispositivo raíz siguen utilizando el mismo volumen de Amazon EBS después de iniciarse en un nuevo host.

Puede establecer el orden del reinicio de la instancia reprogramando la hora de inicio del reinicio de la instancia en https://console.aws.amazon.com/ec2/.

Configuración del mantenimiento del host

Puede configurar el mantenimiento del host para todos los hosts dedicados compatibles mediante AWS Management Console o AWS CLI. Consulte la tabla siguiente para obtener más detalles.

AWS Management Console

Habilitar el mantenimiento del host para su host dedicado mediante AWS Management Console.

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Hosts dedicados (Hosts dedicados).
3. Seleccione el host dedicado > Acciones > Modificar host.
4. Seleccione activar en el campo Mantenimiento del host.

Deshabilitar el mantenimiento del host para su host dedicado mediante AWS Management Console.

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Hosts dedicados (Hosts dedicados).
3. Seleccione el host dedicado > Acciones > Modificar host.
4. Seleccione desactivar en el campo Mantenimiento del host.

Ver la configuración del mantenimento del host de su host dedicado mediante AWS Management Console.

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Hosts dedicados (Hosts dedicados).
3. Seleccione el host dedicado y en la pestaña Descripción, revise el campo Mantenimento del host.

AWS CLI

Habilitar o deshabilitar el mantenimiento del host de su nuevo host dedicado durante la asignación mediante AWS CLI.

Utilice el comando allocate-hosts (asignar hosts).

Habilitado

```
aws ec2 allocate-hosts --region us-east-1 --quantity 1 --instance-type m3.large --
availability-zone us-east-1b --host-maintenance on
```

Deshabilitado

```
aws ec2 allocate-hosts --region us-east-1 --quantity 1 --instance-type m3.large --
availability-zone us-east-1b --host-maintenance off
```

Para habilitar o deshabilitar el mantenimiento del host de su host dedicado existente mediante AWS CLI.

Utilice el comando modify-hosts (modificar hosts).

Habilitado

```
aws ec2 modify-hosts --region us-east-1 --host-maintenance on --host-
ids h-0d123456bbf78910d
```

Deshabilitado

```
aws ec2 modify-hosts --region us-east-1 --host-maintenance off --host-
ids h-0d123456bbf78910d
```

Ver la configuración del mantenimiento del host de un host dedicado mediante AWS CLI.

Utilice el comando describe-hosts.

```
aws ec2 describe-hosts --region us-east-1 --host-ids h-0d123456bbf78910d
```

> **Note**
>
> Si deshabilita el mantenimiento del host, recibirá una notificación por correo electrónico para desalojar el host degradado y migrar manualmente sus instancias a otro host en un plazo de 28 días. Se asigna un host de reemplazo si tiene una reserva de host dedicado. Transcurridos 28 días, las instancias que se ejecutan en el host degradado finalizan y el host se libera automáticamente.

Evento de mantenimiento

Al detectar la degradación, se programa un evento de mantenimiento 14 días después para reiniciar las instancias en un nuevo host dedicado. Recibirá una notificación por correo electrónico con detalles sobre el host degradado, el evento de mantenimiento programado y los intervalos de tiempo de mantenimiento. Para obtener más información, consulte Visualización de eventos programados.

Puede reprogramar el evento de mantenimiento para cualquier día, hasta siete días después de la fecha del evento programado. Para obtener más información sobre la reprogramación, consulte Reprogramación de un evento programado.

El evento de mantenimiento suele tardar algunos minutos en completarse. En el raro caso de que el evento no tenga éxito, recibirá una notificación por correo electrónico para desalojar las instancias del host degradado dentro de un período de tiempo específico.

Estados de mantenimiento del host

Su host dedicado está configurado en el estado `permanent-failure` en el que se detecta la degradación. No puede iniciar instancias en un host dedicado en el estado `permanent-failure`. Al finalizar el evento de mantenimiento, el host degradado se libera y se pone en el estado de `released, permanent-failure`.

Tras detectar la degradación en un host dedicado y antes de programar un evento de mantenimiento, el mantenimiento del host asigna automáticamente un host dedicado de reemplazo a su cuenta.

Este host de reemplazo permanece en un estado `pending` hasta que se programe un evento de mantenimiento. Una vez programado el evento de mantenimiento, el host dedicado de reemplazo pasa al estado `available`.

Puede usar el host dedicado de reemplazo para iniciar nuevas instancias en el host antes del evento de mantenimiento programado. Sin embargo, parte de la capacidad de instancias del host de reemplazo está reservada para las instancias que se deben migrar desde el host degradado. No puede iniciar nuevas instancias en esta capacidad reservada. Para obtener más información, consulte the section called “instancias en hosts dedicados”.

Servicios relacionados

El host dedicado tiene integrado AWS License Manager: realiza un seguimiento de las licencias en sus hosts dedicados de Amazon EC2 (solo se admite en regiones en las que AWS License Manager esté disponible). Para obtener más información, consulte la Guía del usuario de AWS License Manager.

Debe tener suficientes licencias en su Cuenta de AWS para su nuevo host dedicado. Las licencias asociadas a su host degradado se liberan cuando el host se libera una vez finalizado el evento de mantenimiento programado.

Precios

No hay cargos adicionales por usar el mantenimiento del host, pero se aplican los cargos de host dedicado habituales. Para obtener más información, consulte Precios de hosts dedicados de Amazon EC2.

Tan pronto como se inicie el mantenimiento del host, dejará de facturarse el host dedicado degradado. La facturación por el host dedicado de sustitución empieza solo cuando entra en el estado `available`.

Si el host dedicado degradado se facturaba con una tarifa bajo demanda, el host dedicado de reemplazo también se facturará con una tarifa bajo demanda. Si el host dedicado deteriorado tenía una reserva de host dedicado activa, esta se transferirá al host dedicado nuevo.

Realizar el seguimiento de los cambios de configuración

Puede usar AWS Config para registrar cambios en la configuración de hosts dedicados, así como para las instancias que se inician, detienen o terminan en ellos. A continuación, puede usar la información capturada por AWS Config como fuente de datos para los informes de licencias.

AWS Config registra la información de configuración de los hosts dedicados y las instancias individualmente y empareja dicha información a través de relaciones. Existen tres condiciones para la generación de informes:

- AWS Config recording status (Estado de registro): cuando se encuentra On (Activado), AWS Config registra uno o más tipos de recursos de AWS, que pueden incluir hosts dedicados e instancias dedicadas. Para capturar la información necesaria para los informes de licencias, compruebe que los hosts y las instancias se están registrando con los siguientes campos.
- Host recording status (Estado de registro de host): si se establece en Enabled (Habilitado), se registra la información de configuración de los hosts dedicados.
- Instance recording status (Estado de registro de instancia): si se establece en Enabled (Habilitado), se registra la información de configuración de instancias dedicadas.

Si cualquiera de estas tres condiciones está deshabilitada, el icono en el botón Edit Config Recording (Editar registro de configuración) es de color rojo Para sacar el máximo beneficio de esta herramienta, asegúrese de que los tres métodos de registro estén habilitados. Cuando esto sucede, el icono es de color verde. Para editar esta configuración, elija Edit Config Recording (Editar registro de configuración). Se lo dirigirá a la página Set up AWS Config (Configurar) en la consola de AWS Config, donde podrá configurar AWS Config e iniciar el registro de los hosts, las instancias y los demás tipos de recursos admitidos. Para obtener más información, consulte Configuración de AWS Config mediante la consola en la guía para desarrolladores de AWS Config.

> **Note**
>
> AWS Config registra los recursos después de detectarlos, lo que podría tomar varios minutos.

Después de que AWS Config comienza a registrar cambios en la configuración de hosts e instancias, puede conseguir el historial de la configuración de cualquier host que haya asignado o liberado, y de cualquier instancia que haya iniciado, detenido o terminado. Por ejemplo, en cualquier punto en el historial de configuración de un host dedicado, puede buscar cuántas instancias se han iniciado en ese host junto con el número sockets y núcleos que hay en el host. Para cualquiera de esas instancias, también puede buscar el ID de su Imagen de máquina de Amazon (AMI). Puede usar esta información para informar sobre licencias para su propio software enlazado al servidor que tiene licencia por socket o núcleo.

Para ver los historiales de configuración, use cualquiera de las siguientes formas:

- Mediante el uso de la consola de AWS Config. Para cada recurso registrado, puede ver una página de escala de tiempo que proporciona un historial con detalles de la configuración. Para ver esta página, elija el icono gris en la columna Config Timeline (Escala de tiempo de configuración) de la página Dedicated Hosts (Hosts dedicados). Para obtener más información, consulte Visualización de los detalles de la configuración en la consola de AWS Config en la guía para desarrolladores de AWS Config.
- Mediante la ejecución de comandos de la AWS CLI. Primero puede usar el comando list-discovered-resources para obtener una lista con todos los hosts e instancias. A continuación, puede usar el comando get-resource-config-history para obtener detalles de configuración de un host o una instancia para un intervalo de tiempo específico. Para obtener más información, consulte Ver detalles de configuración mediante la CLI en la guía para desarrolladores de AWS Config.
- Mediante el uso de la API de AWS Config en sus aplicaciones. Primero puede usar la acción ListDiscoveredResources para obtener una lista con todos los hosts e instancias. A continuación, puede usar la acción GetResourceConfigHistory para obtener detalles de configuración de un host o una instancia para un intervalo de tiempo específico.

Por ejemplo, para obtener una lista de todos sus hosts dedicados de AWS Config, ejecute un comando de la CLI como el siguiente.

```
aws configservice list-discovered-resources --resource-type AWS::EC2::Host
```

Para obtener el historial de configuración de un host dedicado desde AWS Config, ejecute un comando de la CLI como el siguiente.

```
aws configservice get-resource-config-history --resource-type AWS::EC2::Instance --
resource-id i-1234567890abcdef0
```

Para administrar la configuración de AWS Config mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la página Dedicated Hosts (Hosts dedicados), elija Edit Config Recording (Editar registro de configuración).

3. En la consola de AWS Config, siga los pasos indicados para activar el registro. Para obtener más información, consulte la sección sobre la Configuración de AWS Config mediante la consola.

Para obtener más información, consulte Visualización de los detalles de configuración en la consola de AWS Config.

Para activar AWS Config mediante la línea de comandos o API

- AWS CLI: Visualización de detalles de configuración (AWS CLI) en la Guía para desarrolladores de AWS Config.
- API de Amazon EC2: GetResourceConfigHistory.

Dedicated Instances

De forma predeterminada, las instancias de EC2 se ejecutan en un equipo de tenencia compartida. Esto significa que varias cuentas de AWS pueden compartir el mismo hardware físico.

Las instancias dedicadas son instancias de EC2 que se ejecutan en hardware que está dedicado a una sola cuenta de AWS. Eso significa que las instancias dedicadas están aisladas físicamente en el hardware del host de las instancias que pertenecen a otras Cuentas de AWS, incluso si esas cuentas están vinculadas a la cuenta de un solo pagador. Sin embargo, las instancias dedicadas pueden compartir hardware con otras instancias de la misma Cuenta de AWS que no sean instancias dedicadas.

Las instancias dedicadas no proporcionan visibilidad ni control sobre la ubicación de las instancias, ni admiten la afinidad de host. Si detiene e inicia una instancia dedicada, es posible que no se ejecute en el mismo host. Del mismo modo, no puede dirigirse a un host específico en el que iniciar o ejecutar una instancia. Además, las instancias dedicadas ofrecen compatibilidad limitada con Traiga su propia licencia (BYOL).

Si necesita visibilidad y control sobre la ubicación de las instancias y una compatibilidad con BYOL más completa, considere la posibilidad de utilizar un host dedicado como alternativa. Las instancias dedicadas y los hosts dedicados se pueden utilizar para iniciar instancias de Amazon EC2 en servidores físicos dedicados. No hay diferencias de rendimiento, seguridad o físicas entre las instancias dedicadas y las instancias en hosts dedicados. Sin embargo, hay algunas diferencias clave entre ambos. En la siguiente tabla se enumeran algunas de las principales diferencias entre las instancias dedicadas y los hosts dedicados:

	Host dedicado	Dedicated Instance
Servidor físico dedicado	Servidor físico con capacidad de instancias totalmente dedicado a su uso.	Servidor físico que está dedicado a una sola cuenta de cliente.
Uso compartido de capacidad de instancias	Puede compartir la capacidad de instancias con otras cuentas.	No compatible
Facturación	Facturación por host	Facturación por instancia
Visibilidad de sockets, núcleos e ID de host	Proporciona visibilidad del número de sockets y núcleos físicos	Sin visibilidad
Afinidad de instancia y host	Le permite implementar de forma coherente sus instancias en el mismo servidor físico a lo largo del tiempo	No admitido
Colocación de instancia dirigida	Proporciona visibilidad y control adicional sobre el modo en el que las instancias se colocan en un servidor físico	No admitido
Recuperación automática de instancia	Soportado. Para obtener más informaci ón, consulte Recuperación de host.	Compatible
Bring-Your-Own-License (BYOL)	Compatible	Compatibilidad parcial *
Reservas de capacidad	No compatible	Compatible

* Es posible utilizar Microsoft SQL Server con Movilidad de licencias a través de Software Assurance y licencias de Windows Virtual Desktop Access (VDA) con una instancia dedicada.

Para obtener más información sobre instancias dedicadas, consulte Dedicated Hosts.

Temas

Conceptos básicos de instancia dedicada

Una VPC puede tener una tenencia `default` o `dedicated`. De forma predeterminada, las VPC tienen una tenencia `default` y las instancias iniciadas en una VPC de tenencia `default` tienen una tenencia `default`. Para iniciar instancias dedicadas, haga lo siguiente:

- Cree una VPC con una tenencia `dedicated`, de manera que todas las instancias de la VPC se ejecuten como instancias dedicadas. Para obtener más información, consulte Creación de una VPC con una tenencia de una instancia dedicada.
- Cree una VPC con una tenencia `default` y especifique manualmente una tenencia `dedicated` para que las instancias se ejecuten como instancias dedicadas. Para obtener más información, consulte iniciar instancias dedicadas en una VPC:.

Características admitidas

Las instancias dedicadas admiten las siguientes características e integraciones de servicios de AWS:

Temas

instancias reservadas

Para reservar capacidad para las instancias dedicadas, puede comprar reservas de capacidad o instancias reservadas dedicadas. Para obtener más información, consulte Reserved Instances y On-Demand Capacity Reservations.

Al comprar una instancia reservada dedicada, está adquiriendo la capacidad para iniciar una instancia dedicada en una VPC por una cuota de uso muy reducida; el desglose de precios en el cargo por uso se aplica solo si inicia una instancia con tenencia dedicada. Cuando compra una instancia reservada con una tenencia predeterminada, solo se aplica a una instancia en ejecución con tenencia `default`; no se aplica a una instancia en ejecución con tenencia `dedicated`.

No puede utilizar el proceso de modificación para cambiar la tenencia de la instancia reservada una vez que la haya comprado. Sin embargo, se puede intercambiar una instancia reservada convertible por una instancia reservada convertible nueva con una tenencia diferente.

Escalado automático

Puede utilizar Amazon EC2 Auto Scaling para iniciar instancias dedicadas. Para obtener más información, consulte iniciar instancias de escalado automático en una VPC en la Guía del usuario de Amazon EC2 Auto Scaling.

Recuperación automática

Puede configurar la recuperación automática para las instancias dedicadas que dejan de funcionar debido a un error de equipo subyacente o a un problema que requiera la intervención de AWS para la reparación. Para obtener más información, consulte Resiliencia de las instancias.

instancias de spot dedicado.

Puede ejecutar una instancia de Spot dedicada especificando la tenencia `dedicated` al crear la solicitud de instancia de Spot. Para obtener más información, consulte Especificar una tenencia para su instancias de spot.

Instancias de rendimiento ampliable

Puede aprovechar los beneficios que le brinda utilizar un hardware de tenencia dedicada con the section called “Instancias de rendimiento ampliable”. De forma predeterminada, las instancias dedicadas T3 se inician de modo ilimitado y proporcionan un nivel de referencia del rendimiento de la CPU. Además, pueden ampliarse hasta alcanzar un nivel de CPU superior cuando la carga de trabajo así lo requiera. El rendimiento de referencia de T3 y su capacidad de ampliación se

controlan mediante créditos de CPU. Dada la naturaleza ampliable de los tipos de instancia T3, es recomendable monitorear cómo las instancias T3 utilizan los recursos de CPU del hardware dedicado para obtener el mejor rendimiento. Las instancias dedicadas T3 están pensadas para clientes con cargas de trabajo diversas que muestran un comportamiento aleatorio de la CPU, pero que idealmente tienen un uso medio de la CPU igual o inferior a los usos de referencia. Para obtener más información, consulte the section called “Conceptos clave”.

Amazon EC2 dispone de sistemas para identificar y corregir la variabilidad en el rendimiento. Sin embargo, es posible que se produzca cierta variabilidad a corto plazo si se inician varias instancias dedicadas T3 que tienen patrones de utilización de CPU correlacionados. En el caso de estas cargas de trabajo que están correlacionadas o son más exigentes, recomendamos utilizar instancias dedicadas M5 o M5a en lugar de instancias dedicadas T3.

Limitaciones de instancias dedicadas

Tenga en cuenta las siguientes consideraciones al utilizar las instancias dedicadas:

- Algunos servicios de AWS o sus características no son compatibles con una VPC con la tenencia de instancia establecida en `dedicated`. Consulte la documentación respectiva del servicio para confirmar si existe alguna limitación.
- Algunos tipos de instancias no se pueden iniciar en una VPC con la tenencia de instancia establecida en `dedicated`. Para obtener más información sobre los tipos de instancias admitidos, consulte instancias dedicadas de Amazon EC2.
- Al iniciar una instancia dedicada con respaldo de Amazon EBS, el volumen de EBS no se ejecuta en un equipo de inquilino único.

Precios de las instancias dedicadas

El precio de las instancias dedicadas es distinto del precio de las instancias bajo demanda. Para obtener más información, consulte la página del producto instancias dedicadas de Amazon EC2.

Trabajar con instancias dedicadas

Puede crear una VPC con una tenencia de instancia `dedicated` para garantizar que todas las instancias iniciadas en la VPC son instancias dedicadas. Como alternativa, puede especificar la tenencia de la instancia durante la inicialización.

Temas

Creación de una VPC con una tenencia de una instancia dedicada

Al crear una VPC, tiene la opción de especificar su tenencia de instancia. Si inicia una instancia en una VPC con la tenencia de instancia de `dedicated`, la instancia siempre se ejecutará como una instancia dedicada en el hardware dedicado a su uso.

Para obtener más información sobre cómo crear una VPC y elegir las opciones de tenencia, consulte Creación de una VPC en la Guía del usuario de Amazon VPC.

iniciar instancias dedicadas en una VPC:

Puede iniciar una instancia dedicada con el asistente de inicialización de instancias de Amazon EC2.

Console

Para iniciar una instancia dedicada en una VPC con tenencia predeterminada mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione instancias y elija iniciar instancia.
3. En la sección Application and OS Images (Imágenes de aplicaciones y sistema operativo), seleccione una AMI en la lista.
4. En la sección Instance type (Tipo de instancia), seleccione un tipo de instancia para iniciarla.

> **Note**
>
> Asegúrese de elegir un tipo de instancia que se admita como instancia dedicada. Para obtener más información, consulte Instancias dedicadas de Amazon EC2.

5. En la sección Key pair (Par de claves), seleccione el par de claves para asociarlo con la instancia.

6. En la sección Advanced details (Detalles avanzados), en Tenancy (Tenencia), seleccione Dedicated (Dedicada).
7. Configure las opciones de instancia restantes según sea necesario. Para obtener más información, consulte iniciar una instancia mediante parámetros definidos.
8. Seleccione iniciar instancia.

Command line

Para configurar la opción de tenencia de la instancia durante la inicialización con la línea de comando

- run-instances (AWS CLI)
- New-EC2Instance (AWS Tools for Windows PowerShell)

Para obtener más información acerca de la inicialización de una instancia con una tenencia `host`, consulte iniciar instancias en un host dedicado.

Mostrar información de propiedad

Console

Para mostrar la información de tenencia de la 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 (Sus VPC).
3. Compruebe la tenencia de instancia de su VPC en la columna Tenancy (Propiedad).
4. Si no se muestra la columna Tenencia, elija la configuración () en la esquina superior derecha, active la opción Tenencia y elija Confirmar.

Para mostrar la información de tenencia de la instancia con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Compruebe la tenencia de la instancia en la columna Tenancy (Propiedad).
4. Si no se muestra la columna Tenencia, realice una de las siguientes operaciones:

- Elija la configuración
  ()
  en la esquina superior derecha, active Tenencia y elija Confirmar.
- Seleccione la instancia. En la pestaña Detalles, cerca de la parte inferior de la página, en Host y grupo de ubicación, compruebe el valor de Propiedad.

Command line

Para describir la tenencia de la VPC con la línea de comando

- describe-vpcs (AWS CLI)
- Get-EC2Vpc (AWS Tools for Windows PowerShell)

Para describir la tenencia de la instancia con la línea de comando

- describe-instances (AWS CLI)
- Get-EC2Instance (AWS Tools for Windows PowerShell)

Para describir el valor de tenencia de la instancia reservada con la línea de comando

- describe-reserved-instances (AWS CLI)
- Get-EC2ReservedInstance (AWS Tools for Windows PowerShell)

Para describir el valor de tenencia de la oferta de instancia reservada con la línea de comando

- describe-reserved-instances-offerings (AWS CLI)
- Get-EC2ReservedInstancesOffering (AWS Tools for Windows PowerShell)

Para cambiar la propiedad de una instancia

Puede cambiar la tenencia de una instancia detenida después de iniciarla. Los cambios que realice surtirán efecto la próxima vez que se inicie la instancia.

Los detalles del sistema operativo de la instancia (y si SQL Server está instalado) influyen en las conversiones que se admiten. Para obtener más información sobre las rutas de conversión de

tenencia disponibles para su instancia, consulte Tenancy conversion en la Guía del usuario de License Manager.

> **Note**
>
> En el caso de las instancias T3, debe iniciar la instancia en un host dedicado para poder utilizar una tenencia de `host`. No puede cambiar la tenencia de `host` a `dedicated` o `default`. Al intentar realizar uno de estos cambios de tenencia no admitidos, se produce el código de error `InvalidRequest`.

Console

Para cambiar la tenencia de una instancia con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instancias y seleccione la instancia.
3. Elija Estado de la instancia, Detener instancia,Detener.
4. Elija Actions (Acciones), Instance Settings (Configuración de la instancia) y Modify Instance Placement (Modificar ubicación de la instancia).
5. En Propiedad, elija si desea ejecutar la instancia en hardware dedicado o en un host dedicado. Seleccione Save.

Command line

Para modificar el valor de tenencia de la instancia con la línea de comando

- modify-instance-placement (AWS CLI)
- Edit-EC2InstancePlacement (AWS Tools for Windows PowerShell)

Cambiar la propiedad de una VPC

Puede cambiar la tenencia de la instancia de una VPC de `dedicated` a `default` después de crearla. La modificación de la tenencia de instancia de la VPC no afecta a la tenencia de ninguna de las instancias existentes en la VPC. La siguiente vez que se inicia una instancia en la VPC, posee la tenencia `default`, a menos que se especifique otra durante la inicialización.

> **Note**
>
> No se puede cambiar la propiedad de la instancia de una VPC de `default` a `dedicated` después de crearla.

Solo puede modificar la tenencia de la instancia de una VPC con la AWS CLI, un SDK de AWS o con la API de Amazon EC2.

Command line

Para modificar el atributo de tenencia de instancia de la VPC con AWS CLI

Utilice el comando modify-vpc-tenancy para especificar el ID de la VPC y el valor de la tenencia de la instancia. El único valor admitido es `default`.

```
aws ec2 modify-vpc-tenancy --vpc-id vpc-1a2b3c4d --instance-tenancy default
```

Reservas de capacidad

Las reservas de capacidad le permiten reservar capacidad de cómputo para las instancias de Amazon EC2 en una zona de disponibilidad específica. Existen dos tipos de reservas de capacidad para diferentes casos de uso.

Tipos de reservas de capacidad

- Reservas de capacidad bajo demanda
- bloques de capacidad para ML

A continuación, se indican algunos casos de uso frecuentes de las reservas de capacidad bajo demanda:

- Eventos de escalado: puede crear reservas de capacidad bajo demanda antes de los eventos críticos para la empresa para asegurarse de que pueda escalar cuando lo necesite.
- Requisitos normativos y recuperación de desastres: utilice reservas de capacidad bajo demanda para cumplir con los requisitos reglamentarios de alta disponibilidad y reserve capacidad en una zona de disponibilidad o región diferente para la recuperación de desastres.

A continuación, se indican algunos casos de uso frecuentes de bloques de capacidad para ML:

- Entrenamiento y ajuste de modelos de machine learning (ML): obtenga acceso ininterrumpido a las instancias de GPU que reservó para completar el entrenamiento y el ajuste de los modelos de ML.
- Experimentos y prototipos de ML: ejecute experimentos y cree prototipos que requieran instancias de GPU durante periodos cortos.

Cuándo usar una reserva de capacidad bajo demanda

Utilice las reservas de capacidad bajo demanda si tiene requisitos de capacidad estrictos y ejecuta cargas de trabajo críticas para la empresa que requieren una garantía de capacidad. Con las reservas de capacidad bajo demanda, puede asegurarse de tener siempre acceso a la capacidad de Amazon EC2 que haya reservado durante el tiempo que la necesite.

Cuándo utilizar bloques de capacidad para ML

Use bloques de capacidad para ML cuando necesite asegurarse de tener acceso ininterrumpido a las instancias de GPU durante un periodo de tiempo definido a partir de una fecha futura. bloques de capacidad es un servicio ideal para entrenar y ajustar los modelos de ML, llevar a cabo experimentos cortos y gestionar los aumentos temporales de la demanda de inferencias en el futuro. Con bloques de capacidad, puede asegurarse de tener acceso a los recursos de la GPU en una fecha específica para ejecutar sus cargas de trabajo de ML.

On-Demand Capacity Reservations

Reservas de capacidad bajo demanda le permite reservar capacidad de cómputo para sus instancias de Amazon EC2 en una zona de disponibilidad específica para cualquier duración. Las reservas de capacidad reducen el riesgo de no poder obtener capacidad bajo demanda en caso de que existan restricciones de capacidad. Si tiene requisitos de capacidad estrictos y ejecuta cargas de trabajo críticas para la empresa que requieren cierto nivel de garantía de capacidad a corto o largo plazo, le recomendamos que cree una reserva de capacidad para garantizar que siempre tendrá acceso a la capacidad de Amazon EC2 cuando la necesite y durante el tiempo que la necesite.

Puede crear reservas de capacidad en cualquier momento, sin contraer un compromiso de uno o tres años de plazo. La capacidad está disponible, y la facturación comienza tan pronto como la reserva de capacidad se aprovisiona en su cuenta. Cuando ya no necesite la garantía de capacidad, cancele la reserva de capacidad para que quede liberada y no siga generando gastos. También puede utilizar los descuentos de facturación que ofrecen los Savings Plans y las instancias reservadas regionales para reducir el costo de una reserva de capacidad.

Al crear una Reserva de capacidad, especifica:

- La zona de disponibilidad en la que se reserva la capacidad
- Es el número de instancias para el que debe reservar capacidad
- Los atributos de la instancia, incluido el tipo de instancia, la plataforma, la zona de disponibilidad y la tenencia.

Reservas de capacidad solo pueden usarlas instancias que coincidan con sus atributos. De forma predeterminada, se utilizan de forma automática por instancias en ejecución que coinciden con los atributos. Si no dispone de instancias en ejecución que coincidan con los atributos de Reserva de capacidad, permanecen sin utilizar hasta que inicia una instancia sin atributos que coincidan.

Contenido

Diferencias entre Reservas de capacidad, instancias reservadas y Savings Plans

En la siguiente tabla se indican las principales diferencias entre Reservas de capacidad, instancias reservadas y Savings Plans:

	Capacity Reservations	instancias reservadas de zona	instancias reservadas regionales	Savings Plans
Plazo	Compromiso no necesario. Se pueden crear y cancelar según sea necesario.	Requiere un compromiso establecido de uno o tres años		
Beneficio de capacidad	Capacidad reservada en una zona de disponibilidad específica.		No hay capacidad reservada.	
Descuento de facturación	No hay descuento de facturación. †	Proporciona un descuento de facturación.		
Límites de instancia	Se aplican instancia a petición límites por región.	El valor predeterminado es 20 por zona de disponibilidad. Puede solicitar un aumento del límite.	El valor predeterminado es 20 por región. Puede solicitar un aumento del límite.	Sin límite.

† Puede combinar las reservas de capacidad con Savings Plans o instancias reservadas regionales para recibir un descuento.

Para obtener más información, consulte los siguientes temas:

- Reserved Instances
- Guía de usuario de Savings Plans

Plataformas admitidas

Debe crear la reserva de capacidad con la plataforma adecuada para asegurarse de que se ajuste correctamente con sus instancias. Las reservas de capacidad admiten las siguientes plataformas:

- Linux/UNIX
- Linux con SQL Server Standard
- Linux con SQL Server Web
- Linux con SQL Server Enterprise
- SUSE Linux
- Red Hat Enterprise Linux
- RHEL con SQL Server Standard
- RHEL con SQL Server Enterprise
- RHEL con SQL Server Web
- RHEL con HA
- RHEL con HA y SQL Server Standard
- RHEL con HA y SQL Server Enterprise
- Ubuntu Pro
- Windows
- Windows con SQL Server
- Windows con SQL Server Web
- Windows con SQL Server Standard
- Windows con SQL Server Enterprise

Al adquirir una Reserva de capacidad, debe especificar la plataforma que represente el sistema operativo de la instancia.

- Para las distribuciones de SUSE Linux y RHEL, a excepción de BYOL, debe elegir la plataforma específica. Por ejemplo, la plataforma SUSE Linux o Red Hat Enterprise Linux.
- Para las demás distribuciones de Linux (incluida Ubuntu), elija una plataforma Linux/UNIX.
- Si trae una suscripción RHEL (BYOL) existente, debe elegir la plataforma Linux/UNIX.
- En Windows con SQL Standard, Windows con SQL Server Enterprise y Windows con SQL Server Web, debe elegir las plataformas específicas.

- Para todas las demás versiones de Windows, a excepción de BYOL que no es compatible, elija la plataforma Windows.

Cuotas

El número de instancias permitidas para la reserva de capacidad está basado en la cuota de instancia bajo demanda de su cuenta. Puede reservar capacidad para tantas instancias como permita esa cuota menos el número de instancias que ya se estén ejecutando.

Las cuotas se aplican solo a las instancias en ejecución. Si su instancia está pendiente, en parada, detenida o en hibernación, no se tendrá en cuenta para su cuota.

Limitaciones

Antes de crear Reservas de capacidad, recuerde las siguientes limitaciones y restricciones.

- Recuentos de Reservas de capacidad activas y sin utilizar hacia los límites de instancia a petición.
- No se pueden transferir reservas de capacidad de una cuenta de AWS a otra. Sin embargo, puede compartir reservas de capacidad con otras cuentas de AWS. Para obtener más información, consulte Utilizar Reservas de capacidad compartidas.
- Los descuentos de facturación instancia reservada de zona no se aplican a las Reservas de capacidad.
- Las reservas de capacidad se pueden crear en grupos de ubicación en clúster. No se admiten los grupos de ubicación en particiones y distribución.
- Las Reservas de capacidad no se pueden usar con hosts dedicados. Las reservas de capacidad se pueden usar con instancias dedicadas.
- [Instancias de Windows] Las Reservas de capacidad no se pueden utilizar con Traiga su propia licencia (BYOL).
- Reservas de capacidad no asegura que una instancia hibernada pueda reanudarse después de intentar iniciarla.

Precios y facturación de Reserva de capacidad

Temas

- Precios
- Facturación

- Descuentos de facturación
- Visualización de su factura

Precios

Las reservas de capacidad se cobrarán según la tarifa bajo demanda equivalente, independientemente de que ejecute instancias en la capacidad reservada o no. Si no utiliza la reserva, aparece como una reserva sin utilizar en su factura de Amazon EC2. Cuando se ejecuta una instancia que coincide con los atributos de una reserva, se paga solo por la instancia, no por la reserva. No existen cargos por adelantado ni adicionales.

Por ejemplo, si crea una Reserva de capacidad para las instancias Linux 20 `m4.large` y ejecuta instancias Linux 15 `m4.large` en la misma zona de disponibilidad, se le cobrarán 15 instancias activas y 5 instancias sin usar en la reserva.

Los descuentos de facturación para los Savings Plans y las instancias reservadas regionales se aplican a las Reservas de capacidad. Para obtener más información, consulte Descuentos de facturación.

Para obtener más información, consulte Precios de Amazon EC2.

Facturación

La facturación comienza en cuanto se aprovisiona la reserva de capacidad en su cuenta, y continúa mientras esta permanece aprovisionada en su cuenta.

Las Reservas de capacidad se facturan según el grado de detalle por segundo. Esto significa que se le cobrará por horas parciales. Por ejemplo, si una reserva de capacidad permanece aprovisionada en su cuenta durante 24 horas y 15 minutos, se le cobrarán `24.25` horas de reserva.

En el siguiente ejemplo se muestra cómo se factura una Reserva de capacidad. La Reserva de capacidad se crea para una instancia Linux `m4.large`, que dispone de una tarifa bajo demanda de 0,10 USD por hora de uso. En este ejemplo, la reserva de capacidad se aprovisiona en la cuenta durante cinco horas. La Reserva de capacidad está sin utilizar durante la primera hora, por lo que se cobrará una hora sin utilizar en la tarifa bajo demanda estándar del tipo de instancia `m4.large`. Desde la segunda hora a la quinta, una instancia `m4.large`ocupa la Reserva de capacidad. Durante este tiempo, la Reserva de capacidad no acumula cargos y se factura en la cuenta la instancia `m4.large` que la ocupa. En la sexta hora, la Reserva de capacidad se cancela y la instancia

`m4.large` se ejecuta normalmente fuera de la capacidad reservada. Esa hora se cobra con la tarifa bajo demanda del tipo de instancia `m4.large`.

Hour	1	2	3	4	5	6	Total cost
Unused Capacity Reservation	$0.10	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.10**
On-demand Instance Usage	$0.00	$0.10	$0.10	$0.10	$0.10	$0.10	**$0.50**
Hourly cost	**$0.10**	**$0.10**	**$0.10**	**$0.10**	**$0.10**	**$0.10**	**$0.60**

Descuentos de facturación

Los descuentos de facturación para los Savings Plans y las instancias reservadas regionales se aplican a las Reservas de capacidad. AWS aplica automáticamente estos descuentos a las Reservas de capacidad que tienen atributos coincidentes. Cuando una instancia usa una Reserva de capacidad, el descuento se aplica a la instancia. Los descuentos se aplican preferentemente a las instancias en uso antes que a las Reservas de capacidad sin utilizar.

Los descuentos de facturación de instancias reservadas de zona no se aplican a las Reservas de capacidad.

Para obtener más información, consulte los siguientes temas:

- Reserved Instances
- Guía de usuario de Savings Plans
- Opciones de facturación y compra

Visualización de su factura

Puede revisar los cargos y tarifas aplicados a su cuenta en la consola de AWS Billing and Cost Management.

- El Dashboard (Panel) muestra un resumen de gastos de la cuenta.
- En la página Bills (Facturas), en Details (Detalles), amplíe la sección Elastic Compute Cloud y la región para obtener información sobre la facturación de las Reservas de capacidad.

Puede ver los cargos online o puede descargar un archivo CSV. Para obtener más información, consulte Partidas de reserva de capacidad en la Guía del usuario de AWS Billing and Cost Management.

Utilizar Reservas de capacidad

Para comenzar a utilizar Reservas de capacidad cree la reserva de capacidad en la zona de disponibilidad requerida. A continuación, puede iniciar instancias en la capacidad reservada, ver la utilización de su capacidad en tiempo real y aumentar o disminuir su capacidad según sea necesario.

De forma predeterminada, las Reservas de capacidad coinciden de forma automática con las nuevas instancias e instancias en ejecución que tienen atributos coincidentes (tipo de instancia, plataforma, zona de disponibilidad y tenencia). Esto significa que cualquier instancia con atributos coincidentes se ejecuta automáticamente en la Reserva de capacidad. Sin embargo, también se puede dirigir a una Reserva de capacidad para cargas de trabajo específicas. Esto le permite controlar de manera explícita qué instancias pueden ejecutarse en esa capacidad reservada.

Puede especificar cómo finaliza la reserva. Puede elegir entre cancelar Reserva de capacidad o hacer que finalice de forma automática a una hora especificada. Si especifica una hora de finalización, la Reserva de capacidad se cancela en el plazo de una hora desde el tiempo especificado. Por ejemplo, si especifica 31/5/2019, 13:30:55, se garantiza que la Reserva de capacidad finalice entre las 13:30:55 y las 14:30:55 el 31/5/2019. Una vez una reserva finalice, no podrá destinar instancias a la Reserva de capacidad. Las instancias en ejecución en la capacidad reserva siguen ejecutándose de forma ininterrumpida. Si las instancias que se dirigen a una Reserva de capacidad se detienen, no podrá reiniciarlas hasta que quite la preferencia de destino de la Reserva de capacidad o las configure para que se dirijan a una Reserva de capacidad diferente.

Contenido

Crear una Reserva de capacidad

Si su solicitud de creación de una reserva de capacidad tiene éxito, la capacidad estará disponible de forma inmediata. La capacidad seguirá estando reservada para su uso siempre que la Reserva de capacidad esté activa. Además, podrá iniciar instancias en ella en cualquier momento. Si la Reserva de capacidad está abierta, las instancias nuevas y existentes que tengan atributos coincidentes

se ejecutarán automáticamente en la capacidad de la Reserva de capacidad. Si la Reserva de capacidad tiene el estado `targeted`, las instancias deben dirigirse específicamente a ella para ejecutarse en la capacidad reservada.

Su solicitud para crear una Reserva de capacidad puede fallar si se cumple una de las siguientes:

- Amazon EC2 no tiene suficiente capacidad para llevar a cabo la solicitud. Puede volver a intentarlo más tarde, probar con una zona de disponibilidad distinta o realizar una solicitud inferior. Si su aplicación es flexible en cuanto a los tamaños y tipos de instancia, intente usar atributos de instancia diferentes.
- La cantidad solicitada supera el límite de instancia a petición para la familia de instancias seleccionada. Incremente su límite de instancia a petición para la familia de instancias e inténtelo de nuevo. Para obtener más información, consulte Cuotas de las instancias bajo demanda.

Para crear una Reserva de capacidad con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. Elija Reservas de capacidad y, a continuación, elija Create Reserva de capacidad (Crear Reserva de capacidad).
3. En la página Create a Reserva de capacidad (Crear una Reserva de capacidad), configure los siguientes ajustes en la sección Instance details (Detalles de la instancia): El tipo de instancia, la plataforma, la zona de disponibilidad y la tenencia de las instancias que lance deben coincidir con el tipo de instancia, la plataforma, la zona de disponibilidad y la tenencia que especifique aquí o, de lo contrario, la Reserva de capacidad no se aplicará. Por ejemplo, si una Reserva de capacidad abierta no coincide, un inicialización de instancia que tenga como destino esa Reserva de capacidad producirá un error de forma explícita.

    a. Instance Type (Tipo de instancia) — el tipo de instancia que iniciar en la capacidad reservada.

    b. Launch EBS-optimized instances (iniciar instancias optimizadas para EBS) — especifique si reservar la capacidad para instancias optimizadas para EBS. Esta opción se selecciona de forma predeterminada para algunos tipos de instancias. Para obtener más información, consulte the section called “Optimización de EBS”.

    c. Plataforma — el sistema operativo para sus instancias. Para obtener más información, consulte Plataformas admitidas.

d. Availability Zone (Zona de disponibilidad) — la zona de disponibilidad en la que reservar la capacidad.

e. Tenancy (Tenencia)—especifique si desea ejecutar una instancia de hardware compartido (opción predeterminada) o una instancia dedicada.

f. (Opcional) ARN de grupo de ubicación: el ARN del grupo con ubicación en clúster en el que se debe crear la reserva de capacidad.

   Para obtener más información, consulte Las reservas de capacidad en grupos con ubicación en clúster.

g. Quantity (Cantidad) — el número de instancias para el que reservar capacidad. Si especifica una cantidad que supera el límite de instancia a petición restante para el tipo de instancia seleccionada, se deniega la solicitud.

4. Configure los siguientes ajustes en la sección Reservation details (Detalles de la reserva):

   a. Reservation Ends (Finalizaciones de la reserva) — elija una de las siguientes opciones:

      - Manually (Manualmente) — permite reservar la capacidad hasta que la cancele explícitamente.
      - Specific time (Tiempo específico) — cancela a reserva de capacidad automáticamente en la hora y fecha especificadas.

   b. Instance eligibility (Elegibilidad de la instancia) — elija una de las siguientes opciones.

      - open (abierto) (valor predeterminado): la Reserva de capacidad coincide con cualquier instancia que tiene atributos coincidentes (tipo de instancia, plataforma, zona de disponibilidad y tenencia). Si inicia una instancia con atributos coincidentes, se coloca en la capacidad reservada automáticamente.
      - targeted (dirigido): la Reserva de capacidad solo acepta instancias que tienen atributos coincidentes (tipo de instancia, plataforma, zona de disponibilidad y tenencia), y que se destinan explícitamente a la reserva.

5. Elija Request reservation (Solicitar reserva).

Para crear una reserva de capacidad mediante la AWS CLI

Utilice el comando create-capacity-reservation (crear reserva de capacidad). Para obtener más información, consulte Plataformas admitidas.

El siguiente comando crea una Reserva de capacidad que reserva capacidad para tres instancias `m5.2xlarge` que ejecutan las AMI de Red Hat Enterprise Linux en la zona de disponibilidad `us-east-1a`.

```
aws ec2 create-capacity-reservation --instance-type m5.2xlarge --instance-platform Red
 Hat Enterprise Linux --availability-zone us-east-1a --instance-count 3
```

El comando siguiente crea una Reserva de capacidad que reserva capacidad para tres instancias `m5.2xlarge` que ejecutan Windows con las AMI de SQL Server en la zona de disponibilidad `us-east-1a`.

```
aws ec2 create-capacity-reservation --instance-type m5.2xlarge --instance-
platform Windows with SQL Server --availability-zone us-east-1a --instance-count 3
```

iniciar instancias en una Reserva de capacidad existente

Al iniciar una instancia, puede especificar si desea iniciar la instancia en cualquier Reserva de capacidad `open`, en una Reserva de capacidad determinada o en un grupo de Reservas de capacidad. Solo puede iniciar una instancia en una Reserva de capacidad que tenga atributos coincidentes (tipo de instancia, plataforma, zona de disponibilidad y tenencia) y capacidad suficiente. También puede configurar la instancia para evitar la ejecución en una Reserva de capacidad, incluso si tiene una Reserva de capacidad `open` que tiene atributos coincidentes y capacidad disponible.

la inicialización de una instancia en una Reserva de capacidad reduce su capacidad disponible por número de instancias iniciadas. Por ejemplo, si inicia tres instancias, la capacidad disponible de la Reserva de capacidad se reduce en tres.

Para iniciar instancias en una Reserva de capacidad existente con la consola

1. Siga el procedimiento para iniciar una instancia, pero no la lance hasta que haya completado los siguientes pasos para especificar la configuración del grupo con ubicación y la reserva de capacidad.
2. Expanda Detalles avanzados y haga lo siguiente:

    a. En Grupo de ubicación, seleccione el grupo con ubicación en clúster en el que se iniciará la instancia.

    b. Para Capacity Reservation (Reserva de capacidad), elija una de las siguientes opciones en función de la configuración de la reserva de capacidad:

- Ninguna: impide que las instancias se lancen en un reserva de capacidad. Las instancias se ejecutan en capacidad bajo demanda.
- Abierta: inicia la instancia en cualquier reserva de capacidad que tenga los atributos coincidentes y capacidad suficiente para la cantidad de instancias seleccionadas. Si no hay Reserva de capacidad coincidentes con suficiente capacidad, la instancia se inicia en capacidad bajo demanda.
- Destino por ID: inicia las instancias en la reserva de capacidad seleccionada. Si la Reserva de capacidad seleccionada no tiene suficiente capacidad para la cantidad de instancias seleccionadas, la inicialización de la instancia produce un error.
- Destino por grupo: inicia las instancias en cualquier reserva de capacidad con atributos coincidentes y capacidad disponible en el grupo de reserva de capacidad seleccionado. Si el grupo seleccionado no tiene una Reserva de capacidad con atributos coincidentes y capacidad disponible, las instancias se inician en capacidad bajo demanda.

3. En el panel Summary (Resumen), revise la configuración de la instancia y, a continuación, elija Launch instance (iniciar instancia). Para obtener más información, consulte Lance una instancia con el nuevo asistente de inicialización de instancias.

Para iniciar una instancia en una reserva de capacidad existente mediante la AWS CLI

Utilice el comando run-instances y especifique el parámetro `--capacity-reservation-specification`.

En el siguiente ejemplo se inicia una instancia `t2.micro` en cualquier Reserva de capacidad abierto que cuente con atributos coincidentes y capacidad disponible:

```
aws ec2 run-instances --image-id ami-abc12345 --count 1 --instance-type t2.micro
 --key-name MyKeyPair --subnet-id subnet-1234567890abcdef1 --capacity-reservation-
specification CapacityReservationPreference=open
```

En el siguiente ejemplo se inicia una instancia `t2.micro` en una Reserva de capacidad `targeted`:

```
aws ec2 run-instances --image-id ami-abc12345 --count 1 --instance-type t2.micro
 --key-name MyKeyPair --subnet-id subnet-1234567890abcdef1 --capacity-reservation-
specification CapacityReservationTarget={CapacityReservationId=cr-a1234567}
```

En el siguiente ejemplo se inicia una instancia `t2.micro` en un grupo de Reserva de capacidad:

```
aws ec2 run-instances --image-id ami-abc12345 --count 1
 --instance-type t2.micro --key-name MyKeyPair --subnet-
id subnet-1234567890abcdef1 --capacity-reservation-specification
 CapacityReservationTarget={CapacityReservationResourceGroupArn=arn:aws:resource-
groups:us-west-1:123456789012:group/my-cr-group}
```

Modificar una Reserva de capacidad

Puede cambiar los atributos de una Reserva de capacidad activa después de haberla creado. No puede modificar una Reserva de capacidad después de que haya caducado o después de haberla cancelado explícitamente.

Cuando modifique una Reserva de capacidad, solo puede aumentar o disminuir la cantidad y cambiar la forma en la que se publica. No puede cambiar el tipo de instancia, la optimización para EBS, la plataforma, la zona de disponibilidad ni la elegibilidad de las instancias de una Reserva de capacidad. Si necesita modificar cualquiera de estos atributos, le recomendamos cancelar la reserva y, a continuación, crear una nueva con los atributos obligatorios.

Si especifica una nueva cantidad que supera el límite de instancia a petición restante para el tipo de instancia seleccionada, se producirá un error en la actualización.

Para modificar una Reserva de capacidad con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. Elija Reservas de capacidad, seleccione la Reserva de capacidad que modificar y, a continuación, elija Edit (Editar).
3. Modifique las opciones de Quantity (Cantidad) o Reservation ends (Finalización de la reserva) según corresponda y elija Save changes (Guardar cambios).

Para modificar una reserva de capacidad mediante la AWS CLI

Utilice el comando modify-capacity-reservations:

Por ejemplo, el comando siguiente modifica una Reserva de capacidad para reservar capacidad para ocho instancias.

```
aws ec2 modify-capacity-reservation --capacity-reservation-id cr-1234567890abcdef0 --
instance-count 8
```

Modificar la configuración de la Reserva de capacidad de una instancia

Puede modificar los ajustes de Reserva de capacidad en una instancia detenida en cualquier momento:

- Empiece en cualquier Reserva de capacidad que cuente con atributos coincidentes (tipo de instancia, plataforma, zona de disponibilidad y tenencia) y capacidad disponible.
- Inicie la instancia en un Reserva de capacidad específico.
- Empiece en cualquier Reserva de capacidad que cuente con atributos coincidentes y capacidad disponible en un grupo de Reserva de capacidad
- Evite que la instancia inicie en un Reserva de capacidad.

Para modificar la configuración de la Reserva de capacidad de una instancia con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. Elija Instances (instancia[s]) y, a continuación, seleccione la instancia que desee modificar. Detenga la instancia si aún no está detenida.
3. Seleccione Acciones, Configuración de la instancia, Modificar la configuración de reserva de capacidad.
4. En Reserva de capacidad, elija una de las siguientes opciones:

    - Open (Abrir) — inicia la instancia a cualquier Reserva de capacidad que tenga los atributos correspondientes y capacidad suficiente para la cantidad de instancias seleccionadas. Si no hay Reserva de capacidad coincidentes con suficiente capacidad, la instancia se inicia en capacidad bajo demanda.
    - None (Ninguno) — Hace que las instancias no se lancen en un Reserva de capacidad. Las instancias se ejecutan en capacidad bajo demanda.
    - Specify Capacity Reservation (Especificar reserva de capacidad): inicia las instancias en la Reserva de capacidad seleccionada. Si la Reserva de capacidad seleccionada no tiene suficiente capacidad para la cantidad de instancias seleccionadas, la inicialización de la instancia produce un error.
    - Specify Capacity Reservation group (Especificar grupo de reserva de capacidad): inicia las instancias en cualquier Reserva de capacidad con atributos coincidentes y capacidad disponible en el grupo de Reserva de capacidad seleccionado. Si el grupo seleccionado no tiene una Reserva de capacidad con atributos coincidentes y capacidad disponible, las instancias se inician en capacidad bajo demanda.

Para modificar la configuración de la reserva de capacidad de una instancia mediante la AWS CLI

Utilice el comando modify-instance-capacity-reservation-attributes.

Por ejemplo, el comando siguiente cambia la configuración de Reserva de capacidad de una instancia a `open` o `none`.

```
aws ec2 modify-instance-capacity-reservation-attributes --instance-
id i-1234567890abcdef0 --capacity-reservation-specification
 CapacityReservationPreference=none|open
```

Por ejemplo, el siguiente comando modifica una instancia para dirigirse a una Reserva de capacidad determinada.

```
aws ec2 modify-instance-capacity-reservation-attributes --instance-
id i-1234567890abcdef0 --capacity-reservation-specification
 CapacityReservationTarget={CapacityReservationId=cr-1234567890abcdef0}
```

Por ejemplo, el siguiente comando modifica una instancia para dirigirse a un grupo de Reserva de capacidad determinado.

```
aws ec2 modify-instance-capacity-reservation-attributes --instance-
id i-1234567890abcdef0 --capacity-reservation-specification
 CapacityReservationTarget={CapacityReservationResourceGroupArn=arn:aws:resource-
groups:us-west-1:123456789012:group/my-cr-group}
```

Ver una Reserva de capacidad

Reservas de capacidad tiene los siguientes estados posibles:

- `active` — la capacidad está disponible y se puede utilizar.
- `expired` — la Reserva de capacidad caducó automáticamente en la hora y fecha especificadas en su solicitud de reserva. La capacidad reservada ya no está disponible para su uso.
- `cancelled`—El Reserva de capacidad se ha cancelado. La capacidad reservada ya no está disponible para su uso.
- `pending` — la solicitud de Reserva de capacidad es correcta, pero el aprovisionamiento de la capacidad sigue estando pendiente.

- `failed` — se ha producido un error en la solicitud de Reserva de capacidad. Se puede producir un error en la solicitud debido a parámetros de solicitud no válidos, restricciones de capacidad o restricciones del límite de instancias. Puede ver una solicitud fallida durante 60 minutos.

> **Note**
>
> Debido al modelo de consistencia final que siguen las API de Amazon EC2, después de crear una reserva de capacidad, la consola y la respuesta describe-capacity-reservations pueden tardar hasta 5 minutos en indicar que la reserva de capacidad se encuentra en estado `active`. Durante este tiempo, la consola y la respuesta `describe-capacity-reservations` pueden indicar que la reserva de capacidad se encuentra en estado `pending`. Sin embargo, es posible que la reserva de capacidad ya esté disponible para su uso y pueda intentar iniciar instancias en ella.

Para ver sus Reservas de capacidad con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. Elija Reservas de capacidad y seleccione una Reserva de capacidad que ver.
3. Elija View launched instances for this reservation (Ver instancias iniciadas para esta reserva).

Para ver sus reservas de capacidad mediante la AWS CLI

Utilice el comando describe-capacity-reservations:

Por ejemplo, el comando siguiente describe todas las Reservas de capacidad.

```
aws ec2 describe-capacity-reservations
```

Resultado de ejemplo.

```
{
    "CapacityReservations": [
        {
            "CapacityReservationId": "cr-1234abcd56EXAMPLE ",
            "EndDateType": "unlimited",
            "AvailabilityZone": "eu-west-1a",
            "InstanceMatchCriteria": "open",
```

```
            "Tags": [],
            "EphemeralStorage": false,
            "CreateDate": "2019-08-16T09:03:18.000Z",
            "AvailableInstanceCount": 1,
            "InstancePlatform": "Linux/UNIX",
            "TotalInstanceCount": 1,
            "State": "active",
            "Tenancy": "default",
            "EbsOptimized": true,
            "InstanceType": "a1.medium",
            "PlacementGroupArn": "arn:aws:ec2:us-east-1:123456789012:placement-group/
MyPG"
        },
        {
            "CapacityReservationId": "cr-abcdEXAMPLE9876ef ",
            "EndDateType": "unlimited",
            "AvailabilityZone": "eu-west-1a",
            "InstanceMatchCriteria": "open",
            "Tags": [],
            "EphemeralStorage": false,
            "CreateDate": "2019-08-07T11:34:19.000Z",
            "AvailableInstanceCount": 3,
            "InstancePlatform": "Linux/UNIX",
            "TotalInstanceCount": 3,
            "State": "cancelled",
            "Tenancy": "default",
            "EbsOptimized": true,
            "InstanceType": "m5.large"
        }
    ]
}
```

Cancelar una Reserva de capacidad

Puede cancelar una Reserva de capacidad en cualquier momento si ya no necesita la capacidad reservada. Cuando cancele una Reserva de capacidad, la capacidad se liberará de inmediato y ya no estará reservada para su uso.

Puede cancelar Reservas de capacidad vacías y Reservas de capacidad que tengan instancias en ejecución. Si cancela una Reserva de capacidad que dispone de instancias de ejecución, las instancias siguen ejecutándose de forma normal fuera de la reserva de capacidad con las tarifas de instancia en diferido estándar o con una tarifa con descuento si dispone de un Savings Plan o una instancia reservada regional.

Una vez que cancele una Reserva de capacidad, las instancias a las que se dirigen no pueden volverse a iniciar. Modifique estas instancias de manera que se destinen a un inicialización de Reserva de capacidad, diferente en cualquier Reserva de capacidad con estado open (abierto) con atributos coincidentes y capacidad suficiente, o evite la inicialización en una Reserva de capacidad. Para obtener más información, consulte Modificar la configuración de la Reserva de capacidad de una instancia.

Para cancelar una Reserva de capacidad con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. Elija Reservas de capacidad y seleccione la Reserva de capacidad que cancelar.
3. Elija Cancel reservation (Cancelar reserva) y Cancel reservation (Cancelar reserva).

Para cancelar una reserva de capacidad mediante la AWS CLI

Utilice el comando cancel-capacity-reservation:

Por ejemplo, el siguiente comando cancela una Reserva de capacidad con un ID de `cr-1234567890abcdef0`.

```
aws ec2 cancel-capacity-reservation --capacity-reservation-id cr-1234567890abcdef0
```

Utilizar grupos de Reserva de capacidad

Puede utilizar AWS Resource Groups para crear colecciones lógicas de reservas de capacidad, denominadas resource groups. Un grupo de recursos es una agrupación lógica de recursos de AWS que se encuentran todos en la misma región de AWS. Para obtener más información acerca de los grupos de recursos, consulte ¿Qué son los grupos de recursos? en la Guía del usuario de AWS Resource Groups.

Puede incluir las reservas de capacidad que son de su propiedad en un único grupo de recursos, puede incluir las reservas de capacidad que se comparten con otras cuentas de AWS en un único grupo de recursos. También puede incluir varias reservas de capacidad que tengan atributos diferentes (tipo de instancia, plataforma, zona de disponibilidad y tenencia) en un único grupo de recursos.

Al crear grupos de recursos para reservas de capacidad, puede destinar instancias a un grupo de reservas de capacidad en lugar de a una reserva de capacidad individual. Las instancias destinadas

a un grupo de Reservas de capacidad coinciden con cualquier Reserva de capacidad del grupo que tenga atributos coincidentes (tipo de instancia, plataforma, zona de disponibilidad y tenencia) y capacidad disponible. Si el grupo no tiene una Reserva de capacidad con atributos coincidentes y capacidad disponible, las instancias se ejecutan con capacidad bajo demanda. Si una Reserva de capacidad coincidente se agrega al grupo de destino en una etapa posterior, la instancia coincide automáticamente y se mueve a su capacidad reservada.

Para evitar el uso involuntario de Reservas de capacidad en un grupo, configure las Reservas de capacidad en el grupo para aceptar solo instancias que se dirigen explícitamente a la reserva de capacidad. Para ello, establezca Requisitos de instancia en destino (consola antigua) o Solo instancias que especifican esta reserva (consola nueva) al crear la Reserva de capacidad mediante la consola de Amazon EC2. Cuando utilice AWS CLI, especifique `--instance-match-criteria targeted` al crear la reserva de capacidad. Hacer esto garantiza que solo se pueden ejecutar en el grupo las instancias que se dirigen explícitamente al grupo o a una Reserva de capacidad en el grupo.

Si una Reserva de capacidad en un grupo se cancela o caduca mientras tiene instancias en ejecución, las instancias se mueven automáticamente a otra Reserva de capacidad del grupo que tiene atributos coincidentes y capacidad disponible. Si no queda ningún resto de Reservas de capacidad en el grupo que tenga atributos coincidentes y capacidad disponible, las instancias se ejecutan en capacidad bajo demanda. Si una Reserva de capacidad coincidente se agrega al grupo de destino en una etapa posterior, la instancia se mueve automáticamente a su capacidad reservada.

Temas

Crear un grupo de reservas de capacidad

Para crear un grupo para reservas de capacidad

Utilice el comando de la AWS CLI create-group. Para `name`, proporcione un nombre descriptivo para el grupo y para `configuration`, especifique dos parámetros de solicitud `Type`:

- `AWS::EC2::CapacityReservationPool` para asegurarse de que el grupo de recursos pueda dirigirse para la inicialización de instancias
- `AWS::ResourceGroups::Generic` con `allowed-resource-types` establecido en `AWS::EC2::CapacityReservation` para asegurarse de que el grupo de recursos solo acepta reservas de capacidad

Por ejemplo, el comando siguiente crea un grupo llamado `MyCRGroup`.

```
aws resource-groups create-group --name MyCRGroup --configuration
 '{"Type":"AWS::EC2::CapacityReservationPool"}'
 '{"Type":"AWS::ResourceGroups::Generic", "Parameters": [{"Name": "allowed-resource-
types", "Values": ["AWS::EC2::CapacityReservation"]}]}'
```

A continuación se muestra un resultado de ejemplo.

```
{
    "GroupConfiguration": {
        "Status": "UPDATE_COMPLETE",
        "Configuration": [
            {
                "Type": "AWS::EC2::CapacityReservationPool"
            },
            {
                "Type": "AWS::ResourceGroups::Generic",
                "Parameters": [
                    {
                        "Values": [
                            "AWS::EC2::CapacityReservation"
                        ],
                        "Name": "allowed-resource-types"
                    }
                ]
            }
        ]
    },
    "Group": {
        "GroupArn": "arn:aws:resource-groups:sa-east-1:123456789012:group/MyCRGroup",
        "Name": "MyCRGroup"
    }
}
```

Agregar una reserva de capacidad a un grupo

Si agrega a un grupo una reserva de capacidad compartida con usted, y esa reserva de capacidad no está compartida, se eliminará automáticamente del grupo.

Para agregar una Reserva de capacidad a un grupo

Utilice el comando de la AWS CLI group-resources. Para `group`, especifique el nombre del grupo al que desea agregar Reservas de capacidad y para `resources`, especifique los ARN de las Reservas de capacidad que va a agregar. Para agregar varias Reservas de capacidad, separe los ARN con un espacio. Para los ARN de las Reservas de capacidad que se van a agregar, utilice el comando describe-capacity-reservations (Describir reservas de capacidad) de AWS CLI y especifique los ID de las reservas de capacidad.

Por ejemplo, el comando siguiente agrega dos Reservas de capacidad a un grupo denominado `MyCRGroup`.

```
aws resource-groups group-resources --group MyCRGroup --resource-arns arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1 arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-54321abcdef567890
```

A continuación se muestra un resultado de ejemplo.

```
{
    "Failed": [],
    "Succeeded": [
        "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1",
        "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-54321abcdef567890"
    ]
}
```

Ver las reservas de capacidad en un grupo

Para consultar las Reservas de capacidad en un grupo determinado

Utilice el comando de la AWS CLI list-group-resources. Para `group`, especifique el nombre del grupo.

Por ejemplo, el comando siguiente muestra las Reservas de capacidad en un grupo denominado `MyCRGroup`.

```
aws resource-groups list-group-resources --group MyCRGroup
```

A continuación se muestra un resultado de ejemplo.

```
{
    "QueryErrors": [],
    "ResourceIdentifiers": [
        {
            "ResourceType": "AWS::EC2::CapacityReservation",
            "ResourceArn": "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/
cr-1234567890abcdef1"
        },
        {
            "ResourceType": "AWS::EC2::CapacityReservation",
            "ResourceArn": "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/
cr-54321abcdef567890"
        }
    ]
}
```

> **Note**
>
> La salida del comando incluye reservas de capacidad de su propiedad y reservas de capacidad que se comparten con usted.

Ver los grupos a los que pertenece una reserva de capacidad

AWS CLI

Para ver los grupos a los que se ha agregado una reserva de capacidad concreta

Utilice el comando de la AWS CLI get-groups-for-capacity-reservation.

Por ejemplo, el siguiente comando muestra los grupos a los que se ha agregado Reserva de capacidad `cr-1234567890abcdef1`.

```
aws ec2 get-groups-for-capacity-reservation --capacity-reservation-
id cr-1234567890abcdef1
```

A continuación se muestra un resultado de ejemplo.

```
{
    "CapacityReservationGroups": [
        {
            "OwnerId": "123456789012",
            "GroupArn": "arn:aws:resource-groups:sa-east-1:123456789012:group/
MyCRGroup"
        }
    ]
}
```

> **Note**
>
> Si especifica una reserva de capacidad que se comparte con usted, el comando solo devuelve los grupos de reserva de capacidad de los que es propietario.

Amazon EC2 console

Para ver los grupos a los que se ha agregado una reserva de capacidad concreta

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Reservas de capacidad, seleccione la Reserva de capacidad que desea consultar y, a continuación, elija View (Ver).

   Los grupos a los que se ha agregado Reserva de capacidad se muestran en la tarjeta Groups (Grupos).

> **Note**
>
> Si elige una reserva de capacidad que se comparte con usted, la consola solo devuelve los grupos de reserva de capacidad de los que es propietario.

Para eliminar una reserva de capacidad de un grupo

Para eliminar una Reserva de capacidad de un grupo

Utilice el comando de la AWS CLI ungroup-resources. Para `group`, especifique el ARN del grupo del que desea quitar la Reserva de capacidad y para `resources` especifique los ARN de las Reservas

de capacidad que desea quitar. Para quitar varias Reservas de capacidad, separe los ARN con un espacio.

En el ejemplo siguiente se quitan dos Reservas de capacidad de un grupo denominado `MyCRGroup`.

```
aws resource-groups ungroup-resources --group MyCRGroup --resource-arns arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-0e154d26a16094dd arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-54321abcdef567890
```

A continuación se muestra un resultado de ejemplo.

```
{
    "Failed": [],
    "Succeeded": [
        "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-0e154d26a16094dd",
        "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-54321abcdef567890"
    ]
}
```

Eliminar un grupo de reservas de capacidad

Para eliminar un grupo

Utilice el comando de la AWS CLI delete-group. Para `group`, proporcione el nombre del grupo que desea eliminar.

Por ejemplo, el siguiente comando elimina un grupo denominado `MyCRGroup`.

```
aws resource-groups delete-group --group MyCRGroup
```

A continuación se muestra un resultado de ejemplo.

```
{
    "Group": {
        "GroupArn": "arn:aws:resource-groups:sa-east-1:123456789012:group/MyCRGroup",
        "Name": "MyCRGroup"
    }
}
```

Las reservas de capacidad en grupos con ubicación en clúster

Puede crear reservas de capacidad en un grupo con ubicación en clúster para reservar la capacidad de computación de Amazon EC2 para sus cargas de trabajo. Los grupos de ubicación en clústeres ofrecen el beneficio de una baja latencia de red y un alto rendimiento de red.

La creación de una reserva de capacidad en un grupo con ubicación en clúster garantiza que tenga acceso a la capacidad de computación en los grupos de ubicación en clúster cuando la necesite, durante el tiempo que la necesite. Esto es ideal para reservar capacidad para cargas de trabajo de alto rendimiento (HPC) que requieren escalado de computación. Le permite reducir la escala del clúster a la vez que garantiza que la capacidad permanezca disponible para su uso, de modo que pueda escalar de nuevo cuando sea necesario.

Temas

Limitaciones

Tenga en cuenta lo siguiente al crear reservas de capacidad en grupos de ubicación en clúster:

- Si una reserva de capacidad existente no se encuentra en un grupo con ubicación, no puede modificar la reserva de capacidad para reservar capacidad en un grupo con ubicación. Para reservar capacidad en un grupo de ubicación, debe crear la reserva de capacidad en el grupo de ubicación.
- Después de crear una reserva de capacidad en un grupo de ubicación, no puede modificarla para reservar capacidad fuera del grupo de ubicación.
- Puede aumentar la capacidad reservada en un grupo de ubicación al modificar una reserva de capacidad existente en el grupo de ubicación o crear reservas de capacidad adicionales en el grupo de ubicación. Sin embargo, aumenta las probabilidades de que se produzca un error de capacidad insuficiente.
- No puede compartir reservas de capacidad creadas en un grupo con ubicación en clúster.
- No se puede eliminar un grupo con ubicación en clúster que tenga reservas de capacidad `active`. Debe cancelar todas las reservas de capacidad en el grupo con ubicación en clúster antes de poder eliminarlo.

Trabajar con reservas de capacidad en grupos de ubicación en clúster

Para empezar a utilizar reservas de capacidad con grupos de ubicación en clúster, lleve a cabo los siguientes pasos.

> **Note**
>
> Si desea crear una reserva de capacidad en un grupo con ubicación en clúster existente, omita el paso 1. A continuación, en los pasos 2 y 3, especifique el ARN del grupo con ubicación en clúster existente. Para obtener más información acerca de cómo buscar el ARN de su grupo con ubicación en clúster existente, consulte Visualización de información de los grupos con ubicación.

Temas

Paso 1: (Condicional) Cree un grupo con ubicación en clúster para utilizarlo con una reserva de capacidad

Realice este paso únicamente si necesita crear un nuevo grupo con ubicación en clúster. Para utilizar un grupo con ubicación en clúster existente, omita este paso y, a continuación, en los pasos 2 y 3, utilice el ARN de ese grupo con ubicación en clúster. Para obtener más información acerca de cómo buscar el ARN de su grupo con ubicación en clúster existente, consulte Visualización de información de los grupos con ubicación.

Puede crear un grupo con ubicación en clúster mediante uno de los siguientes métodos.

Console

Para crear un grupo con ubicación en clúster mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Placement Groups (Grupos de ubicación) y luego elija Create Placement Group (Crear grupo de ubicación).

3. Para Name (Nombre), especifique un nombre descriptivo para el grupo de ubicación.
4. Para Placement strategy (Estrategia de ubicación), elija Cluster (Clúster).
5. Elija Crear grupo.
6. En la tabla Grupos de ubicación, en la columna ARN del grupo, tome nota del ARN del grupo con ubicación en clúster que creó. Lo necesitará para el siguiente paso.

AWS CLI

Para crear un grupo con ubicación en clúster con la AWS CLI

Utilice el comando create-placement-group. Para `--group-name`, especifique un nombre descriptivo para el grupo de ubicación y para `--strategy`, especifique `cluster`.

En el ejemplo siguiente se crea un grupo de ubicación denominado `MyPG` que utiliza la estrategia de ubicación `cluster`.

```
aws ec2 create-placement-group \
    --group-name MyPG \
    --strategy cluster
```

Anote el ARN del grupo de ubicación devuelto en la salida del comando, ya que lo necesitará en el paso siguiente.

Paso 2: crear una reserva de capacidad en un grupo con ubicación en clúster

Puede crear una reserva de capacidad en un grupo con ubicación en clúster del mismo modo que crea cualquier reserva de capacidad. Sin embargo, también debe especificar el ARN del grupo con ubicación en clúster en el que se va a crear la reserva de capacidad. Para obtener más información, consulte Crear una Reserva de capacidad.

Consideraciones

- El grupo con ubicación en clúster especificado debe tener el estado `available`. Si el grupo con ubicación en clúster se encuentra en el estado `pending`,`deleting`, o `deleted`, la solicitud falla.
- La reserva de capacidad y el grupo con ubicación en clúster deben estar en la misma zona de disponibilidad. Si la solicitud de creación de la reserva de capacidad especifica una zona de disponibilidad distinta de la del grupo con ubicación en clúster, la solicitud falla.

- Puede crear reservas de capacidad solo para tipos de instancia admitidos por grupos de ubicación en clúster. Si especifica un tipo de instancia no compatible, la solicitud falla. Para obtener más información, consulte Reglas y limitaciones de los grupos de ubicación en clúster.
- Si crea una reserva de capacidad `open` en un grupo con ubicación en clúster y existen instancias de ejecución que tienen atributos coincidentes (ARN del grupo de ubicación, tipo de instancia, zona de disponibilidad, plataforma y tenencia), esas instancias se ejecutan automáticamente en la reserva de capacidad.
- Su solicitud para crear una Reserva de capacidad puede fallar si se cumple una de las siguientes:
  - Amazon EC2 no tiene suficiente capacidad para llevar a cabo la solicitud. Puede volver a intentarlo más tarde, probar con una zona de disponibilidad distinta o usar una capacidad menor. Si su carga de trabajo es flexible en cuanto a los tamaños y tipos de instancia, intente utilizar atributos de instancia diferentes.
  - La cantidad solicitada supera el límite de instancia a petición para la familia de instancias seleccionada. Incremente su límite de instancia a petición para la familia de instancias e inténtelo de nuevo. Para obtener más información, consulte Cuotas de las instancias bajo demanda.

Puede crear la reserva de capacidad en el grupo con ubicación en clúster mediante uno de los siguientes métodos.

Console

Para crear una Reserva de capacidad con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. Elija Reservas de capacidad y, a continuación, elija Create Reserva de capacidad (Crear Reserva de capacidad).
3. En la página Crear una reserva de capacidad, especifique el tipo de instancia, la plataforma, la zona de disponibilidad, la tenencia, la cantidad y la fecha de finalización según sea necesario.
4. En Grupo de ubicación, seleccione el ARN del grupo con ubicación en clúster en el que se creará la reserva de capacidad.
5. Seleccione Crear.

Para obtener más información, consulte Crear una Reserva de capacidad.

AWS CLI

Para crear una reserva de capacidad mediante la AWS CLI

Utilice el comando create-capacity-reservation (crear reserva de capacidad). Para `--placement-group-arn`, especifique el ARN del grupo con ubicación en clúster en el que se creará la reserva de capacidad.

```
$ aws ec2 create-capacity-reservation \
    --instance-type instance_type \
    --instance-platform platform \
    --availability-zone az \
    --instance-count quantity \
    --placement-group-arn placement_group_ARN
```

Para obtener más información, consulte Crear una Reserva de capacidad.

Paso 3: lance las instancias en el grupo con ubicación en clúster

inicia una instancia en una reserva de capacidad en un grupo con ubicación en clúster del mismo modo que inicia una instancia en cualquier reserva de capacidad. Sin embargo, también debe especificar el ARN del grupo con ubicación en clúster en el que iniciar la instancia. Para obtener más información, consulte Crear una Reserva de capacidad.

Consideraciones

- Si la reserva de capacidad es `open`, no es necesario especificar la reserva de capacidad en la solicitud de inicialización de instancia. Si la instancia tiene atributos (ARN del grupo de ubicación, tipo de instancia, zona de disponibilidad, plataforma y tenencia) que coinciden con una reserva de capacidad en el grupo de ubicación especificado, la instancia se ejecuta automáticamente en la reserva de capacidad.
- Si la reserva de capacidad solo acepta inicializacións de instancias segmentadas, debe especificar la reserva de capacidad de destino además del grupo con ubicación en clúster de la solicitud.
- Si la reserva de capacidad está en un grupo de reserva de capacidad, debe especificar el grupo de reserva de capacidad de destino además del grupo con ubicación en clúster en la solicitud. Para obtener más información, consulte Utilizar grupos de Reserva de capacidad.

Puede iniciar una instancia en una reserva de capacidad en un grupo con ubicación en clúster mediante uno de los siguientes métodos.

Console

Para iniciar instancias en una Reserva de capacidad existente con la consola

1. Siga el procedimiento para iniciar una instancia, pero no la lance hasta que haya completado los siguientes pasos para especificar la configuración del grupo con ubicación y la reserva de capacidad.
2. Expanda Detalles avanzados y haga lo siguiente:
   a. En Grupo de ubicación, seleccione el grupo con ubicación en clúster en el que se iniciará la instancia.
   b. Para Capacity Reservation (Reserva de capacidad), elija una de las siguientes opciones en función de la configuración de la reserva de capacidad:
      - Abierta: para iniciar las instancias en cualquier reserva de capacidad `open` en el grupo con ubicación en clúster que tiene atributos coincidentes y capacidad suficiente.
      - Destino por ID: para iniciar las instancias en una reserva de capacidad que solo acepta inicializacións de instancias dirigidas.
      - Destino por grupo: para iniciar las instancias en cualquier reserva de capacidad con atributos coincidentes y capacidad disponible en el grupo de reserva de capacidad seleccionado.
3. En el panel Summary (Resumen), revise la configuración de la instancia y, a continuación, elija Launch instance (iniciar instancia). Para obtener más información, consulte Lance una instancia con el nuevo asistente de inicialización de instancias.

Para obtener más información, consulte iniciar instancias en una Reserva de capacidad existente.

AWS CLI

iniciar instancias en una reserva de capacidad existente mediante la AWS CLI

Utilice el comando run-instances. Si necesita dirigirse a una reserva de capacidad específica o a un grupo de reserva de capacidad, especifique el parámetro `--capacity-reservation-specification`. Para `--placement`, especifique el parámetro `GroupName` y, a continuación, especifique el nombre del grupo de ubicación que creó en los pasos anteriores.

El siguiente comando inicia una instancia en una reserva de capacidad `targeted` en un grupo con ubicación en clúster.

```
$ aws ec2 run-instances \
    --image-id ami_id \
    --count quantity \
    --instance-type instance_type \
    --key-name key_pair_name \
    --subnet-id subnetid \
    --capacity-reservation-specification
 CapacityReservationTarget={CapacityReservationId=capacity_reservation_id} \
    --placement "GroupName=cluster_placement_group_name"
```

Para obtener más información, consulte iniciar instancias en una Reserva de capacidad existente.

Reservas de capacidad en Local Zones

Una zona local es una extensión de una región de AWS que está geográficamente cerca de sus usuarios. Los recursos creados en una zona local pueden prestar servicio a los usuarios locales con comunicaciones de muy baja latencia. Para obtener más información, consulte AWS Local Zones.

Puede extender una VPC desde su región de AWS principal a una zona local mediante la creación de una nueva subred en esa zona local. Cuando crea una subred en una zona local, la VPC también se amplía a dicha zona local. La subred de la zona local funciona igual que otras subredes de la VPC.

Mediante el uso de Local Zones, puede aplicar Reservas de capacidad en varias ubicaciones más cercanas a los usuarios. Las Reservas de capacidad en Local Zones se crean y utilizan de la misma manera que se crean y utilizan las Reservas de capacidad en zonas de disponibilidad normales. Se aplican las mismas características y el mismo comportamiento de asignación de instancias. Para obtener más información acerca de los modelos de precios admitidos en Local Zones, consulte Preguntas frecuentes sobre Local Zones de AWS.

Consideraciones

No puede usar grupos de reserva de capacidad en una zona local.

Para utilizar una reserva de capacidad en una zona local

1. Habilite la zona local para utilizarla en la cuenta de AWS. Para obtener más información, consulte Optar por Local Zones.
2. Cree una reserva de capacidad en la zona local. En la Availability Zone (Zona de disponibilidad), elija la zona local. Una zona local se representa mediante un código de región de AWS seguido

de un identificador que indica la ubicación, por ejemplo, `us-west-2-lax-1a`. Para obtener más información, consulte Crear una Reserva de capacidad.

3. Cree una subred en la zona local. En la Availability Zone (Zona de disponibilidad), elija la zona local. Para obtener más información, consulte Creación de una subred en la VPC en la Guía del usuario de Amazon VPC.
4. Lance una instancia. En la Subnet (Subred), elija la subred de Wavelength (por ejemplo `subnet-123abc | us-west-2-lax-1a`) y, en la Capacity Reservation (Reserva de capacidad), elija la especificación (`open` o según el ID) necesaria para la Reserva de capacidad que creó en la Wavelength. Para obtener más información, consulte iniciar instancias en una Reserva de capacidad existente.

Reservas de capacidad en zonas Wavelength

AWS Wavelength permite a los desarrolladores crear aplicaciones que ofrecen una latencia extremadamente baja para dispositivos móviles y usuarios finales. Wavelength implementa servicios de computación y almacenamiento de AWS estándar al borde de redes 5G de operadores de telecomunicaciones. Puede ampliar una Amazon Virtual Private Cloud (VPC) a una o varias zonas Wavelength. A continuación, puede utilizar recursos de AWS, como instancias de Amazon EC2, para ejecutar aplicaciones que requieren latencia ultrabaja y una conexión a servicios de AWS en la región. Para obtener más información, consulte Zonas de AWS Wavelength.

Al crear una Reservas de capacidad bajo demanda, puede elegir la zona de Wavelength y puede iniciar instancias en una Reserva de capacidad en una zona Wavelength al especificar la subred asociada a la zona Wavelength. Una zona Wavelength se representa mediante un código de región de AWS seguido de un identificador que indica la ubicación, por ejemplo, `us-east-1-wl1-bos-wlz-1`.

Las zonas de Wavelength no están disponibles en todas las regiones. Para obtener información sobre las regiones que admiten zonas de Wavelength, consulte Zonas de Wavelength disponibles en la Guía para desarrolladores de AWS Wavelength.

Consideraciones

No puede usar grupos de Reserva de capacidad en una zona Wavelength.

Utilizar una Reserva de capacidad en una zona Wavelength

1. Habilite la zona Wavelength para utilizarla en la cuenta de AWS. Para obtener más información, consulte the section called “Habilitar zonas de Wavelength”.

2. Crear una Reserva de capacidad en la zona Wavelength. En la Availability Zone (Zona de disponibilidad), elija la Wavelength. Una Wavelength se representa mediante un código de región de AWS seguido de un identificador que indica la ubicación, por ejemplo, `us-east-1-wl1-bos-wlz-1`. Para obtener más información, consulte Crear una Reserva de capacidad.
3. Crear una subred en la zona Wavelength. En la Availability Zone (Zona de disponibilidad), elija la zona Wavelength. Para obtener más información, consulte Creación de una subred en la VPC en la Guía del usuario de Amazon VPC.
4. Lance una instancia. En la Subnet (Subred), elija la subred de Wavelength (por ejemplo `subnet-123abc | us-east-1-wl1-bos-wlz-1`) y, en la Reserva de capacidad, elija la especificación (`open` o según el ID) necesaria para la Reserva de capacidad que creó en la Wavelength. Para obtener más información, consulte iniciar instancias en una Reserva de capacidad existente.

Reservas de capacidad en AWS Outposts

AWS Outposts es un servicio completamente administrado que extiende la infraestructura, los servicios, las API y las herramientas de AWS a las instalaciones del cliente. Al proporcionar acceso local a la infraestructura administrada de AWS, AWS Outposts habilita a los clientes a crear y ejecutar aplicaciones en las instalaciones mediante el uso de las mismas interfaces de programación que en las regiones de AWS, al mismo tiempo que utilizan recursos informáticos y de almacenamiento locales para reducir la latencia y las necesidades de procesamiento de datos locales.

Un Outpost es un grupo de capacidad informática y de almacenamiento de AWS implementada en un sitio del cliente. AWS opera, supervisa y administra esta capacidad como parte de una región de AWS.

Puede crear reservas de capacidad en Outposts que haya creado en su cuenta. Esto le permite reservar capacidad de cómputo en un Outpost en su sitio. Las reservas de capacidad en Outposts se crean y utilizan de la misma manera que se crean y utilizan las reservas de capacidad en zonas de disponibilidad normales. Se aplican las mismas características y el mismo comportamiento de asignación de instancias.

También puede compartir reservas de capacidad en Outposts con otras cuentas de AWS de su organización mediante AWS Resource Access Manager. Para obtener información sobre cómo compartir reservas de capacidad, consulte Utilizar Reservas de capacidad compartidas.

Requisito previo

Debe tener un Outpost instalado en su sitio. Para obtener más información, consulte Crear una instancia de Outpost y solicitar capacidad de Outpost en la Guía del usuario de AWS Outposts.

Consideraciones

- No puede usar grupos de reserva de capacidad en un Outpost.

Para usar una reserva de capacidad en un Outpost

1. Cree una subred en el Outpost. Para obtener más información, consulte Crear una subred en la Guía del usuario de AWS Outposts.
2. Cree una reserva de capacidad en el Outpost.
   a. Abra la consola de AWS Outposts en https://console.aws.amazon.com/outposts/.
   b. En el panel de navegación, elija Outposts, luego haga clic en Actions (Acciones), Create Capacity Reservation (Crear reserva de capacidad).
   c. Configure la reserva de capacidad según sea necesario y, a continuación, elija Create. (Crear) Para obtener más información, consulte Crear una Reserva de capacidad.

   > **Note**
   >
   > La lista desplegable de los Tipos de instancias muestra solo los tipos de instancias que son compatibles con el Outpost seleccionado y la lista desplegable de zonas de disponibilidad muestra solo la zona de disponibilidad con la que está asociado el Outpost seleccionado.

3. Lance una instancia en la reserva de capacidad. Para Subnet (Subred)elija la subred que ha creado en el paso 1, y paraCapacity Reservation (Reserva de capacidad), seleccione la reserva de capacidad que ha creado en el paso 2. Para obtener más información, consulte Lanzar una instancia en Outpost en la Guía del usuario de AWS Outposts.

Utilizar Reservas de capacidad compartidas

El uso compartido de reservas de capacidad permite a los propietarios de reservas de capacidad compartir su capacidad reservada con otras cuentas de AWS o dentro de una organización de AWS. Esto le permite crear y administrar las reservas de capacidad de forma centralizada y compartir la capacidad reservada entre varias cuentas de AWS o dentro de su organización de AWS.

En este modelo, la cuenta de AWS que posee la reserva de capacidad (propietario) la comparte con otras dos cuentas de AWS (consumidores). Los consumidores pueden iniciar instancias en Reservas de capacidad que comparten con ellos de la misma forma que harían con las Reservas de capacidad que poseen en su propia cuenta. El propietario de la Reserva de capacidad es responsable de administrar la Reserva de capacidad y las instancias que inician en la misma. Los propietarios no pueden modificar instancias que los consumidores inician en Reservas de capacidad que han compartido. Los consumidores son responsables de administrar las instancias que inician en Reservas de capacidad compartidas con ellos. Los consumidores no pueden ver o modificar instancias propiedad de otros consumidores o del propietario de la Reserva de capacidad.

Un propietario de una Reserva de capacidad puede compartir una Reserva de capacidad con:

- Cuentas específicas de AWS dentro o fuera de su organización de AWS
- Una unidad organizativa dentro de su organización de AWS
- Toda su organización de AWS

Contenido

Requisitos previos para compartir Reservas de capacidad

- Para compartir una reserva de capacidad, debe poseerla en su cuenta de AWS. No puede compartir una Reserva de capacidad que se ha compartido con usted.
- Solo puede compartir Reservas de capacidad para instancias de tenencia compartida. No puede compartir Reservas de capacidad para instancias de tenencia dedicada.

- El uso compartido de reservas de capacidad no está disponible para nuevas cuentas de AWS o cuentas de AWS que tengan un historial de facturación limitado.
- Para compartir reservas de capacidad con su organización de AWS o una unidad organizativa en su organización de AWS, debe habilitar el uso compartido con AWS Organizations. Para obtener más información, consulte Habilitar el uso compartido con AWS Organizations en la Guía del usuario de AWS RAM.

Servicios relacionados

El uso compartido de reservas de capacidad se integra con AWS Resource Access Manager (AWS RAM). AWS RAM es un servicio que le permite compartir sus recursos de AWS con cualquier cuenta de AWS o a través de AWS Organizations. Con AWS RAM, puede compartir recursos de su propiedad creando un uso compartido de recursos. Un uso compartido de recursos especifica los recursos que compartir y los consumidores con quienes compartirlos. Los consumidores pueden ser cuentas de AWS individuales, unidades organizativas o toda una organización de AWS Organizations.

Para obtener más información sobre AWS RAM, consulte la Guía del usuario de AWS RAM.

Compartir el uso entre zonas de disponibilidad

Para garantizar que los recursos se distribuyen por todas las zonas de disponibilidad de una región, asignamos zonas de disponibilidad de manera independiente a nombres de cada cuenta. Esto podría dar lugar a diferencias de nomenclatura de zona de disponibilidad entre cuentas. Por ejemplo, es posible que la zona de disponibilidad `us-east-1a` de su cuenta de AWS no se encuentre en la misma ubicación de `us-east-1a` que otra cuenta de AWS.

Para identificar la ubicación de las Reservas de capacidad relativa a las cuentas, debe utilizar el ID de zona de disponibilidad (ID de AZ). El ID de AZ es un identificador único y coherente para una zona de disponibilidad en todas las cuentas de AWS. Por ejemplo, `use1-az1` es un ID de AZ para la región `us-east-1` y está en la misma ubicación en todas las cuentas de AWS.

Para ver los ID de AZ para las zonas de disponibilidad de su cuenta

1. Abra la consola de AWS RAM en https://console.aws.amazon.com/ram.
2. Los ID de AZ de la región actual se muestran en el panel Your AZ ID (Su ID de AZ) en el lado derecho de la pantalla.

Compartir una Reserva de capacidad

Al compartir una reserva de capacidad que posee con otras cuentas de AWS, las habilita para iniciar instancias en su capacidad reservada. Si comparte una Reserva de capacidad abierta, tenga en cuenta lo siguiente dado que podría dar lugar a un uso de Reserva de capacidad no intencionado:

- Si los consumidores tienen instancias en ejecución que coinciden con los atributos de la Reserva de capacidad, tienen el parámetro `CapacityReservationPreference` establecido en `open` y no se están ejecutando todavía en capacidad reservada, utilizan automáticamente la Reserva de capacidad compartida.
- Si los consumidores inician instancias que tienen atributos coincidentes (tipo de instancia, plataforma, zona de disponibilidad y tenencia) y tienen el parámetro `CapacityReservationPreference` definido en `open`, se inician automáticamente en la Reserva de capacidad compartida.

Para compartir una Reserva de capacidad, debe añadirla a un uso compartido de recursos. Un uso compartido de recursos es un recurso de AWS RAM que le permite compartir los recursos a través de cuentas de AWS. Un uso compartido de recursos especifica los recursos que compartir y los consumidores con quienes se comparten. Cuando se comparte una Reserva de capacidad, utilizando la consola de Amazon EC2, la añade a un uso compartido de recurso existente. Para agregar la reserva de capacidad a un nuevo uso compartido de recurso, debe crear el uso compartido del recurso mediante la consola de AWS RAM.

Si forma parte de una organización de AWS Organizations y en ella está habilitado el uso compartido, a los consumidores de la organización se les concede acceso a la reserva de capacidad compartida si se cumplen los requisitos previos de uso compartido. Si la reserva de capacidad se comparte con cuentas externas, reciben una invitación para unirse al recurso compartido y se les concede acceso a la reserva de capacidad compartida después de aceptar la invitación.

> **Important**
>
> Antes de iniciar instancias en una reserva de capacidad que se comparta con usted, verifique que tiene acceso a la reserva de capacidad compartida visualizándola en la consola o describiéndola mediante el comando de la AWS CLI describe-capacity-reservations. Si puede ver la reserva de capacidad compartida en la consola o describirla mediante la AWS CLI, está disponible para su uso y puede iniciar instancias en ella. Si intenta iniciar instancias en

la reserva de capacidad y no se puede acceder a ella debido a un error de uso compartido, las instancias se iniciarán en capacidad bajo demanda.

Puede compartir una reserva de capacidad que posea mediante la consola de Amazon EC2, la consola de AWS RAM o la AWS CLI.

Cómo compartir una Reserva de capacidad que posea utilizando la consola de Amazon EC2

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Reservas de capacidad.
3. Elija la Reserva de capacidad para compartir y seleccione Actions (Acciones), Share reservation (Compartir reserva).
4. Seleccione el uso compartido al que añadir la Reserva de capacidad y elija Share Reserva de capacidad (Compartir Reserva de capacidad).

   Los consumidores pueden tardar algunos minutos en obtener acceso a la Reserva de capacidad compartida.

Para compartir una reserva de capacidad que posea mediante la consola de AWS RAM

Consulte Crear un recurso compartido en la Guía del usuario de AWS RAM.

Para compartir una reserva de capacidad que posea mediante la AWS CLI

Utilice el comando create-resource-share.

Dejar de compartir una Reserva de capacidad

El propietario del Reserva de capacidad puede dejar de compartir un Reserva de capacidad en cualquier momento. Se aplican las siguientes reglas:

- Las instancias propiedad de los consumidores que se estaban ejecutando en la capacidad compartida en el momento de dejar de compartirlas se siguen ejecutando con normalidad fuera de la capacidad reservada y la capacidad se restaura a la Reserva de capacidad, dependiendo de la disponibilidad de capacidad de Amazon EC2.
- Los consumidores con quienes se compartió la Reserva de capacidad ya no inician nuevas instancias en la capacidad reservada.

Para dejar de compartir un Reserva de capacidad de su propiedad, debe quitarlo del recurso compartido. Para ello, puede utilizar la consola de Amazon EC2, la consola de AWS RAM o la AWS CLI.

Para dejar de compartir un Reserva de capacidad de su propiedad mediante la consola de Amazon EC2

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Reservas de capacidad.
3. Seleccione el Reserva de capacidad y elija la pestaña Sharing (Compartir).
4. La pestaña Sharing (Uso compartido) muestra los usos compartidos de recursos a los que se ha añadido la Reserva de capacidad. Seleccione el uso compartido de recurso desde el que desea quitar la Reserva de capacidad y elija Remove from resource share (Quitar de recurso compartido).

Para dejar de compartir una reserva de capacidad que posea mediante la consola de AWS RAM

Consulte Actualizar un recurso compartido en la Guía del usuario de AWS RAM.

Para dejar de compartir una reserva de capacidad que posea mediante la AWS CLI

Utilice el comando disassociate-resource-share.

Identificar y visualizar una reserva de capacidad compartida

> **Important**
>
> Antes de iniciar instancias en una reserva de capacidad que se comparta con usted, verifique que tiene acceso a la reserva de capacidad compartida visualizándola en la consola o describiéndola mediante la AWS CLI. Si puede ver la reserva de capacidad compartida en la consola o describirla mediante la AWS CLI, está disponible para su uso y puede iniciar instancias en ella. Si intenta iniciar instancias en la reserva de capacidad y no se puede acceder a ella debido a un error de uso compartido, las instancias se iniciarán en capacidad bajo demanda.

Los propietarios y consumidores pueden identificar y visualizar reservas de capacidad compartidas mediante la consola de Amazon EC2 y la AWS CLI.

Cómo identificar una Reserva de capacidad compartida utilizando la consola de Amazon EC2

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Reservas de capacidad. La pantalla muestras las Reservas de capacidad que posee y las Reservas de capacidad que se comparten con usted. La columna Owner (Propietario) muestra el ID de cuenta de AWS del propietario de la reserva de capacidad. El `(me)` junto al ID de cuenta de AWS indica que usted es el propietario.

Para identificar una reserva de capacidad compartida mediante la AWS CLI

Utilice el comando describe-capacity-reservations: El comando devuelve las reservas de capacidad que son de su propiedad y las reservas de capacidad que se comparten con usted. El `OwnerId` muestra el ID de cuenta de AWS del propietario de la reserva de capacidad.

Ver el uso de la Reserva de capacidad compartido

El propietario de una reserva de capacidad compartida puede consultar su uso en cualquier momento mediante la consola de Amazon EC2 y la AWS CLI.

Cómo ver la Reserva de capacidad mediante la consola de Amazon EC2

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Reservas de capacidad.
3. Seleccione la Reserva de capacidad para la que desea consultar el uso y elija la pestaña Usage (Uso).

   La columna AWS account ID (ID de cuenta de) muestra los ID de cuenta de los consumidores que en la actualidad utilizan la reserva de capacidad. La columna Launched instances (instancias iniciadas) muestra el número de instancias que está ejecutando actualmente cada consumidor en la capacidad reservada.

Para ver el uso de la reserva de capacidad mediante la AWS CLI

Utilice el comando get-capacity-reservation-usage. `AccountId` muestra el ID de cuenta de la cuenta que utiliza la Reserva de capacidad. `UsedInstanceCount` muestra el número de instancias que el consumidor actualmente está ejecutando en la capacidad reservada.

Permisos de una Reserva de capacidad compartida

Permisos de los propietarios

Los propietarios tienen la responsabilidad de administrar y cancelar sus Reservas de capacidad compartidas Los propietarios no pueden modificar instancias que se ejecuten en la Reserva de capacidad compartida que sean propiedad de otras cuentas. Los propietarios siguen siendo responsables de administrar las instancias que inician en la Reserva de capacidad compartida.

Permisos de los consumidores

Los consumidores son responsables de administrar sus instancia que ejecutan la Reserva de capacidad compartida. Los consumidores no pueden modificar la Reserva de capacidad compartida en modo alguno y no pueden ver o modificar instancias que son propiedad de otros consumidores o del propietario de Reserva de capacidad.

Facturación y medición

No hay recargos adicionales para compartir Reservas de capacidad.

Al propietario de la Reserva de capacidad se le facturan las instancias que ejecutan dentro de la Reserva de capacidad y para la capacidad reservada sin utilizar. Se factura a los consumidores las instancias que ejecutan dentro de la Reserva de capacidad compartida.

Si el propietario de la reserva de capacidad pertenece a una cuenta de pago diferente y la reserva de capacidad está cubierta por una instancia reservada regional o un plan de Savings Plans, al propietario de la reserva de capacidad se le seguirán facturando cualquiera de los dos. En estos casos, el propietario de la reserva de capacidad paga la instancia reservada regional o el plan de Savings Plans. Además, a los consumidores se les facturan las instancias que se ejecutan en la reserva de capacidad compartida.

Límites de instancias

Todo el uso de Reserva de capacidad se tiene en cuenta en los límites de instancia a petición del propietario de la Reserva de capacidad. Esto incluye:

- Capacidad reservada sin utilizar
- Uso de instancias del propietario de la Reserva de capacidad
- Uso de instancias propiedad de los consumidores

Las instancias iniciadas en la capacidad compartida por los consumidores se tienen en cuenta en el límite de instancia a petición del propietario de la Reserva de capacidad. Los límites de instancia de los consumidores son una suma de sus propios límites de instancia bajo demanda y la capacidad disponible en las reservas de capacidad compartidas a las que tienen acceso.

Flotas de reservas de capacidad

Una Flota de reserva de capacidad en diferido es un grupo de Reservas de capacidad.

Una solicitud de Flota de Reservas de capacidad contiene toda la información de configuración necesaria para iniciar una Flota de Reservas de capacidad. Con una única solicitud puede reservar grandes cantidades de capacidad de Amazon EC2 para su carga de trabajo en varios tipos de instancias, hasta la capacidad de destino que especifique.

Después de crear una Flota de Reservas de capacidad puede administrar las Reservas de capacidad de la flota de forma colectiva, modificando o cancelando la Flota de Reservas de capacidad.

Temas

Cómo funcionan las Flotas de Reservas de capacidad

Al crear una Flota de Reservas de capacidad, la flota intenta crear Reservas de capacidad individuales y cumplir la capacidad de destino total que haya especificado en la solicitud de flota.

El número de instancias para las que la flota reserva capacidad depende de la capacidad de destino total y de las ponderaciones de tipo de instancia que se especifiquen. El tipo de instancia para el que reserva capacidad depende de la estrategia de asignación y de las prioridades del tipo de instancia que se utilicen.

Si no hay suficiente capacidad en el momento de crear la flota y no puede cumplir inmediatamente su capacidad de destino total, la flota intenta crear Reservas de capacidad asíncronas hasta que haya reservado la cantidad de capacidad solicitada.

Cuando la flota alcanza su capacidad de destino total, intenta mantener esa capacidad. Si se cancela una reserva de capacidad de la flota, esta crea automáticamente una o más Reservas de capacidad, según la configuración de la flota, para reemplazar la capacidad perdida y mantener su capacidad de destino total.

Las Reservas de capacidad de la flota no se pueden administrar individualmente. Deben administrarse colectivamente modificando la flota. Al modificar una flota, las Reservas de capacidad de la flota se actualizan automáticamente para reflejar los cambios.

Actualmente, las flotas de Reservas de capacidad admiten los criterios `open` de asignación de instancias, y todas las Reservas de capacidad iniciadas por una flota utilizan automáticamente estos criterios de asignación de instancias. Con estos criterios, las nuevas instancias e instancias existentes que tienen atributos coincidentes (tipo de instancia, plataforma, zona de disponibilidad y tenencia) se ejecutan automáticamente en las Reservas de capacidad creadas por la flota. Las flotas de reserva de capacidad no admiten criterios `target` de asignación de instancias.

Consideraciones

Tenga en cuenta lo siguiente cuando trabaje con flotas de Reservas de capacidad:

- Se puede crear, modificar, ver y cancelar una Flota de Reservas de capacidad mediante la AWS CLI y la API de AWS.
- Las Reservas de capacidad de una flota no se pueden administrar individualmente. Deben administrarse colectivamente modificando o cancelando la flota.
- Una Flota de Reservas de capacidad no puede abarcar distintas regiones.
- Una Flota de Reservas de capacidad no puede abarcar distintas zonas de disponibilidad.
- Las Reservas de capacidad creadas por una Flota de Reservas de capacidad se etiquetan automáticamente con la siguiente etiqueta generada por AWS:
  - Clave: `aws:ec2-capacity-reservation-fleet`
  - Value: *`fleet_id`*

  Puede utilizar esta etiqueta para identificar las Reservas de capacidad creadas por una Flota de Reservas de capacidad.

Precios

No hay recargos adicionales para usar flotas de Reservas de capacidad. Se le facturan las Reservas de capacidad individuales creadas por sus flotas de Reservas de capacidad. Para obtener información acerca de cómo se facturan las Reservas de capacidad, consulte Precios y facturación de Reserva de capacidad.

Conceptos de Flota de Reservas de capacidad

En este tema se describen algunos de los conceptos de las flotas de Reservas de capacidad.

Temas

- Capacidad de destino total
- Estrategia de asignación
- Ponderación de tipo de instancias
- Prioridad de tipo de instancias

Capacidad de destino total

La capacidad de destino total es la cantidad total de capacidad informática que reserva la Flota de Reservas de capacidad. Especifique la capacidad de destino total cuando cree la Flota de Reservas de capacidad. Una vez creada la flota, Amazon EC2 crea automáticamente Reservas de capacidad para reservar capacidad hasta la capacidad de destino total.

El número de instancias para las que la Flota de Reservas de capacidad reserva capacidad se determina por la capacidad de destino total y las ponderaciones de tipo de instancia que especifique para cada tipo de instancia en la Flota de Reservas de capacidad (`total target capacity/instance type weight=number of instances`).

Puede asignar una capacidad de destino total en función de las unidades que sean significativas para su carga de trabajo. Por ejemplo, si su carga de trabajo requiere un cierto número de vCPU, puede asignar la capacidad de destino total en función del número de vCPU necesarias. Si su carga de trabajo requiere `2048` vCPU, especifique una capacidad de destino total de `2048`, y luego asigne ponderaciones de tipo de instancia en función del número de vCPU proporcionadas por los tipos de instancia de la flota. Para ver un ejemplo, consulte Ponderación de tipo de instancias.

Estrategia de asignación

La estrategia de asignación de la Flota de Reservas de capacidad determina cómo se atiende la solicitud de capacidad reservada a partir de las especificaciones de tipo de instancia en la configuración de la Flota de Reservas de capacidad.

En la actualidad, solo se admite la estrategia de asignación `prioritized`. Con esta estrategia, la Flota de Reservas de capacidad crea Reservas de capacidad utilizando las prioridades que ha asignado a cada una de las especificaciones de tipo de instancia en la configuración de la Flota de Reservas de capacidad. Los valores de prioridad más bajos indican mayor prioridad para su uso. Por ejemplo, supongamos que crea una Flota de Reservas de capacidad que utiliza los siguientes tipos de instancia y prioridades:

- `m4.16xlarge`: prioridad = 1
- `m5.16xlarge`: prioridad = 3
- `m5.24xlarge`: prioridad = 2

Primero la flota intenta crear Reservas de capacidad para `m4.16xlarge`. Si Amazon EC2 no tiene suficiente capacidad de `m4.16xlarge`, la flota intenta crear Reservas de capacidad para `m5.24xlarge`. Si Amazon EC2 no tiene suficiente capacidad de `m5.24xlarge`, la flota intenta crear Reservas de capacidad para `m5.16xlarge`.

Ponderación de tipo de instancias

La ponderación de tipo de instancias es una ponderación asignada a cada tipo de instancia de la Flota de Reservas de capacidad. La ponderación determina con cuántas unidades de capacidad cuenta cada instancia de ese tipo de instancia específico con relación a la capacidad de destino total de la flota.

Puede asignar las ponderaciones en función de las unidades que sean significativas para su carga de trabajo. Por ejemplo, si su carga de trabajo requiere cierto número de vCPU, puede asignar ponderaciones en función del número de vCPU proporcionadas por cada tipo de instancia en la Flota de Reservas de capacidad. En este caso, si crea una Flota de Reservas de capacidad con instancias `m4.16xlarge` y `m5.24xlarge`, asignaría ponderaciones que correspondan al número de vCPU para cada instancia de la siguiente manera:

- `m4.16xlarge`: 64 vCPU, ponderación = 64 unidades
- `m5.24xlarge`: 96 vCPU, ponderación = 96 unidades

La ponderación del tipo de instancia determina el número de instancias para las que reserva capacidad la Flota de Reservas de capacidad. Por ejemplo, si una Flota de Reservas de capacidad con una capacidad de destino total de 384 unidades utiliza los tipos de instancia y las ponderaciones del ejemplo anterior, la flota podría reservar capacidad para 6 instancias `m4.16xlarge` (capacidad de destino de 384/ponderación de tipo de instancia de 64 = 6 instancias) o 4 instancias `m5.24xlarge` (384/96 = 4).

Si no asigna ponderaciones de tipo de instancia o si asigna una ponderación de tipo de instancia de 1, la capacidad de destino total se basa únicamente en el recuento de instancias. Por ejemplo, si una Flota de Reservas de capacidad con una capacidad de destino total de 384 unidades utiliza los tipos de instancia del ejemplo anterior, pero omite las ponderaciones o especifica una ponderación de 1 para ambos tipos de instancias, la flota podría reservar capacidad para 384 instancias `m4.16xlarge` o bien para 384 instancias `m5.24xlarge`.

Prioridad de tipo de instancias

La prioridad de tipo de instancias es un valor que asigna a los tipos de instancias de la flota. Las prioridades se utilizan para determinar cuáles de los tipos de instancias especificados para la flota deben priorizarse para su uso.

Los valores de prioridad más bajos indican una prioridad superior para su uso.

Utilizar flotas de Reservas de capacidad

Temas

Antes de empezar

Antes de crear una Flota de Reservas de capacidad:

1. Determine la cantidad de capacidad informática que necesita su carga de trabajo.

2. Decida los tipos de instancia y las zonas de disponibilidad que desea utilizar.
3. Asigne prioridad a cada tipo de instancia en función de sus necesidades y preferencias. Para obtener más información, consulte Prioridad de tipo de instancias.
4. Cree un sistema de ponderación de capacidad que tenga sentido para su carga de trabajo. Asigne una ponderación a cada tipo de instancia y determine la capacidad de destino total. Para obtener más información, consulte Ponderación de tipo de instancias y Capacidad de destino total.
5. Determine si necesita la reserva de capacidad indefinidamente o solo durante un período de tiempo específico.

Estados de las Flota de Reservas de capacidad

Una Flota de Reservas de capacidad puede tener uno de los siguientes estados:

- `submitted`: se ha enviado la solicitud de Flota de Reservas de capacidad y Amazon EC2 se está preparando para crear las Reservas de capacidad.
- `modifying`: se está modificando la Flota de Reservas de capacidad. La flota permanece en este estado hasta que se complete la modificación.
- `active`: la Flota de Reservas de capacidad ha atendido su capacidad de destino total y está intentando mantener esta capacidad. La solicitud permanece en este estado hasta que se modifica o se elimina.
- `partially_fulfilled`: la Flota de Reservas de capacidad ha atendido parcialmente su capacidad de destino total. No hay suficiente capacidad de Amazon EC2 para atender la capacidad de destino total. La flota está intentando atender de forma asíncrona su capacidad de destino total.
- `expiring`: la Flota de Reservas de capacidad ha llegado a su fecha de finalización y está en proceso de caducidad. Es posible que una o más de sus Reservas de capacidad sigan activas.
- `expired`: la Flota de Reservas de capacidad ha llegado a su fecha de finalización. La flota y sus Reservas de capacidad han caducado. La flota no puede crear nuevas Reservas de capacidad.
- `cancelling`: la Flota de Reservas de capacidad está en proceso de cancelarse. Es posible que una o más de sus Reservas de capacidad sigan activas.
- `cancelled`: la Flota de Reservas de capacidad se ha cancelado manualmente. La flota y sus Reservas de capacidad se cancelan y la flota no puede crear nuevas Reservas de capacidad.
- `failed`: la Flota de Reservas de capacidad no pudo reservar capacidad para los tipos de instancias especificados.

Crear una Flota de Reservas de capacidad

Cuando crea una Flota de Reservas de capacidad, crea automáticamente Reservas de capacidad para los tipos de instancias especificados en la solicitud de flota, hasta la capacidad de destino total especificada. El número de instancias para las que la flota reserva capacidad depende de la capacidad de destino total y de las ponderaciones de tipo de instancia que especifique en la solicitud. Para obtener más información, consulte Ponderación de tipo de instancias y Capacidad de destino total.

Al crear la flota, debe especificar los tipos de instancias que se van a utilizar y una prioridad para cada uno de esos tipos de instancias. Para obtener más información, consulte Estrategia de asignación y Prioridad de tipo de instancias.

> **Note**
>
> El rol vinculado a servicio AWSServiceRoleForEC2CapacityReservationFleet se crea automáticamente en su cuenta la primera vez que cree una Flota de Reservas de capacidad. Para obtener más información, consulte Uso de roles vinculados a servicios para la flota de reservas de capacidad.

Las flotas de Reservas de capacidad solo admiten los criterios `open` de asignación de instancias.

Puede crear una Flota de Reservas de capacidad utilizando únicamente la línea de comandos.

Para crear una Flota de Reservas de capacidad

Utilice el comando create-capacity-reservation-fleet de la AWS CLI.

```
aws ec2 create-capacity-reservation-fleet \
--total-target-capacity capacity_units \
--allocation-strategy prioritized \
--instance-match-criteria open \
--tenancy dedicated|default \
--end-date yyyy-mm-ddThh:mm:ss.000Z \
--instance-type-specifications file://instanceTypeSpecification.json
```

A continuación, se muestra el contenido de `instanceTypeSpecification.json`.

```
[
```

```
    {
        "InstanceType": "instance_type",
        "InstancePlatform":"platform",
        "Weight": instance_type_weight,
        "AvailabilityZone":"availability_zone",
        "AvailabilityZoneId" : "az_id",
        "EbsOptimized": true|false,
        "Priority" : instance_type_priority
    }
]
```

Resultado previsto.

```
{
    "Status": "status",
    "TotalFulfilledCapacity": fulfilled_capacity,
    "CapacityReservationFleetId": "cr_fleet_id",
    "TotalTargetCapacity": capacity_units
}
```

Ejemplo

```
aws ec2 create-capacity-reservation-fleet \
--total-target-capacity 24 \
--allocation-strategy prioritized \
--instance-match-criteria open \
--tenancy default \
--end-date 2021-12-31T23:59:59.000Z \
--instance-type-specifications file://instanceTypeSpecification.json
```

`instanceTypeSpecification.json`

```
[
  {
    "InstanceType": "m5.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "Weight": 3.0,
    "AvailabilityZone":"us-east-1a",
    "EbsOptimized": true,
    "Priority" : 1
  }
]
```

Resultado de ejemplo.

```
{
    "Status": "submitted",
    "TotalFulfilledCapacity": 0.0,
    "CapacityReservationFleetId": "crf-abcdef01234567890",
    "TotalTargetCapacity": 24
}
```

Ver una Flota de Reservas de capacidad

Puede ver la información de configuración y capacidad de una Flota de Reservas de capacidad en cualquier momento. La visualización de una flota también proporciona detalles sobre las Reservas de capacidad individuales que se encuentran dentro de la flota.

Puede ver una Flota de Reservas de capacidad utilizando únicamente la línea de comandos.

Para ver una Flota de Reservas de capacidad

Utilice el comando describe-capacity-reservation-fleets de la AWS CLI.

```
aws ec2 describe-capacity-reservation-fleets \
--capacity-reservation-fleet-ids cr_fleet_ids
```

Resultado previsto

```
{
    "CapacityReservationFleets": [
        {
            "Status": "status",
            "EndDate": "yyyy-mm-ddThh:mm:ss.000Z",
            "InstanceMatchCriteria": "open",
            "Tags": [],
            "CapacityReservationFleetId": "cr_fleet_id",
            "Tenancy": "dedicated|default",
            "InstanceTypeSpecifications": [
                {
                    "CapacityReservationId": "cr1_id",
                    "AvailabilityZone": "cr1_availability_zone",
                    "FulfilledCapacity": cr1_used_capacity,
                    "Weight": cr1_instance_type_weight,
                    "CreateDate": "yyyy-mm-ddThh:mm:ss.000Z",
```

```
                    "InstancePlatform": "cr1_platform",
                    "TotalInstanceCount": cr1_number of instances,
                    "Priority": cr1_instance_type_priority,
                    "EbsOptimized": true|false,
                    "InstanceType": "cr1_instance_type"
                },
    {
                    "CapacityReservationId": "cr2_id",
                    "AvailabilityZone": "cr2_availability_zone",
                    "FulfilledCapacity": cr2_used_capacity,
                    "Weight": cr2_instance_type_weight,
                    "CreateDate": "yyyy-mm-ddThh:mm:ss.000Z",
                    "InstancePlatform": "cr2_platform",
                    "TotalInstanceCount": cr2_number of instances,
                    "Priority": cr2_instance_type_priority,
                    "EbsOptimized": true|false,
                    "InstanceType": "cr2_instance_type"
                },
            ],
            "TotalTargetCapacity": total_target_capacity,
            "TotalFulfilledCapacity": total_target_capacity,
            "CreateTime": "yyyy-mm-ddThh:mm:ss.000Z",
            "AllocationStrategy": "prioritized"
        }
    ]
}
```

Ejemplo

```
aws ec2 describe-capacity-reservation-fleets \
--capacity-reservation-fleet-ids crf-abcdef01234567890
```

Resultado de ejemplo

```
{
    "CapacityReservationFleets": [
        {
            "Status": "active",
            "EndDate": "2021-12-31T23:59:59.000Z",
            "InstanceMatchCriteria": "open",
            "Tags": [],
            "CapacityReservationFleetId": "crf-abcdef01234567890",
            "Tenancy": "default",
```

```
            "InstanceTypeSpecifications": [
                {
                    "CapacityReservationId": "cr-1234567890abcdef0",
                    "AvailabilityZone": "us-east-1a",
                    "FulfilledCapacity": 5.0,
                    "Weight": 1.0,
                    "CreateDate": "2021-07-02T08:34:33.398Z",
                    "InstancePlatform": "Linux/UNIX",
                    "TotalInstanceCount": 5,
                    "Priority": 1,
                    "EbsOptimized": true,
                    "InstanceType": "m5.xlarge"
                }
            ],
            "TotalTargetCapacity": 5,
            "TotalFulfilledCapacity": 5.0,
            "CreateTime": "2021-07-02T08:34:33.397Z",
            "AllocationStrategy": "prioritized"
        }
    ]
}
```

Modificar una Flota de Reservas de capacidad

Puede modificar la capacidad de destino total y la fecha de una Flota de Reservas de capacidad en cualquier momento. Al modificar la capacidad de destino total de una Flota de Reservas de capacidad, la flota crea automáticamente nuevas Reservas de capacidad o modifica o cancela las Reservas de capacidad existentes en la flota para cumplir la nueva capacidad de destino total. Al modificar la fecha de finalización de la flota, las fechas de finalización de todas las Reservas de capacidad individuales se actualizan en consecuencia.

Después de modificar una flota, su estado pasa a `modifying`. No puede intentar realizar modificaciones adicionales en una flota mientras esté en el estado `modifying`.

No puede modificar la tenencia, la zona de disponibilidad, los tipos de instancia, las plataformas de instancias, las prioridades ni las ponderaciones utilizadas por una Flota de Reservas de capacidad. Si necesita cambiar cualquiera de estos parámetros, puede que deba cancelar la flota existente y crear una nueva con los parámetros necesarios.

Puede modificar una Flota de Reservas de capacidad utilizando únicamente la línea de comandos.

Para modificar una Flota de Reservas de capacidad

Utilice el comando modify-capacity-reservation-fleet de la AWS CLI.

> **Note**
>
> No puede especificar `--end-date` y `--remove-end-date` en el mismo comando.

```
aws ec2 modify-capacity-reservation-fleet \
--capacity-reservation-fleet-id cr_fleet_ids \
--total-target-capacity capacity_units \
--end-date yyyy-mm-ddThh:mm:ss.000Z \
--remove-end-date
```

Resultado previsto

```
{
    "Return": true
}
```

Ejemplo: Modificación de la capacidad de destino total

```
aws ec2 modify-capacity-reservation-fleet \
--capacity-reservation-fleet-id crf-01234567890abcedf \
--total-target-capacity 160
```

Ejemplo: Modificación de la fecha de finalización

```
aws ec2 modify-capacity-reservation-fleet \
--capacity-reservation-fleet-id crf-01234567890abcedf \
--end-date 2021-07-04T23:59:59.000Z
```

Ejemplo: Eliminación de la fecha de finalización

```
aws ec2 modify-capacity-reservation-fleet \
--capacity-reservation-fleet-id crf-01234567890abcedf \
--remove-end-date
```

Ejemplo de resultado

```
{
```

```
    "Return": true
}
```

Cancelar una Flota de Reservas de capacidad

Cuando ya no necesite una Flota de Reservas de capacidad y la capacidad que dicha flota reserva, puede cancelarla. Al cancelar una flota, su estado cambia a `cancelled` y ya no puede crear nuevas Reservas de capacidad. Además, se cancelan todas las Reservas de capacidad individuales de la flota y las instancias que se estaban ejecutando anteriormente en la capacidad reservada siguen funcionando normalmente en capacidad compartida.

Puede cancelar una Flota de Reservas de capacidad utilizando únicamente la línea de comandos.

Para cancelar una Flota de Reservas de capacidad

Utilice el comando cancel-capacity-reservation-fleet de la AWS CLI.

```
aws ec2 cancel-capacity-reservation-fleets \
--capacity-reservation-fleet-ids cr_fleet_ids
```

Resultado previsto

```
{
    "SuccessfulFleetCancellations": [
        {
            "CurrentFleetState": "state",
            "PreviousFleetState": "state",
            "CapacityReservationFleetId": "cr_fleet_id_1"
        },
        {
            "CurrentFleetState": "state",
            "PreviousFleetState": "state",
            "CapacityReservationFleetId": "cr_fleet_id_2"
        }
    ],
    "FailedFleetCancellations": [
        {
         "CapacityReservationFleetId": "cr_fleet_id_3",
         "CancelCapacityReservationFleetError": [
             {
              "Code": "code",
                    "Message": "message"
```

```
          }
         ]
     }
    ]
}
```

Ejemplo: Cancelación satisfactoria

```
aws ec2 cancel-capacity-reservation-fleets \
--capacity-reservation-fleet-ids crf-abcdef01234567890
```

Ejemplo de resultado

```
{
    "SuccessfulFleetCancellations": [
        {
            "CurrentFleetState": "cancelling",
            "PreviousFleetState": "active",
            "CapacityReservationFleetId": "crf-abcdef01234567890"
        }
    ],
    "FailedFleetCancellations": []
}
```

Ejemplo de configuraciones de Flota de Reservas de capacidad

Temas

- Ejemplo 1: Reserva de capacidad basada en vCPU

Ejemplo 1: Reserva de capacidad basada en vCPU

En el siguiente ejemplo se crea una Flota de Reservas de capacidad que utiliza dos tipos de instancia: `m5.4xlarge` y `m5.12xlarge`.

Utiliza un sistema de ponderación basado en el número de vCPU proporcionadas por los tipos de instancias especificados. La capacidad de destino total es `480` vCPU. La instancia `m5.4xlarge` proporciona 16 vCPU y obtiene una ponderación de 16, mientras que la instancia `m5.12xlarge` proporciona 48 vCPU y obtiene una ponderación de 48. Este sistema de ponderación configura la Flota de Reservas de capacidad para que reserve capacidad para 30 instancias `m5.4xlarge` (480/16=30) o bien para 10 instancias `m5.12xlarge` (480/48=10).

La flota está configurada para priorizar la capacidad de `m5.12xlarge` y obtiene una prioridad de 1, mientras que `m5.4xlarge` obtiene una prioridad inferior, de 2. Esto significa que la flota intentará reservar primero la capacidad de `m5.12xlarge` y solo intentará reservar la capacidad de `m5.4xlarge` si Amazon EC2 no tiene suficiente capacidad de `m5.12xlarge`.

La flota reserva la capacidad para instancias `Windows` y la reserva caduca automáticamente el `October 31, 2021` a las `23:59:59` UTC.

```
aws ec2 create-capacity-reservation-fleet \
--total-target-capacity 480 \
--allocation-strategy prioritized \
--instance-match-criteria open \
--tenancy default \
--end-date 2021-10-31T23:59:59.000Z \
--instance-type-specifications file://instanceTypeSpecification.json
```

A continuación, se muestra el contenido de `instanceTypeSpecification.json`.

```
[
    {
        "InstanceType": "m5.4xlarge",
        "InstancePlatform":"Windows",
        "Weight": 16,
        "AvailabilityZone":"us-east-1a",
        "EbsOptimized": true,
        "Priority" : 2
    },
    {
        "InstanceType": "m5.12xlarge",
        "InstancePlatform":"Windows",
        "Weight": 48,
        "AvailabilityZone":"us-east-1a",
        "EbsOptimized": true,
        "Priority" : 1
 }
]
```

Uso de roles vinculados a servicios para la flota de reservas de capacidad

La Flota de Reservas de capacidad en diferido utiliza roles vinculados a servicios de AWS Identity and Access Management(IAM)https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_terms-and-concepts.html#iam-term-service-linked-role. Un rol vinculado a servicio es un tipo único de rol de

IAM que está vinculado directamente a una Flota de Reservas de capacidad. Los roles vinculados a servicios los predefine la Flota de Reservas de capacidad e incluyen todos los permisos que el servicio necesita para llamar a otros servicios de AWS en su nombre.

Un rol vinculado a servicio simplifica la configuración de la Flota de Reservas de capacidad porque ya no tendrá que agregar manualmente los permisos necesarios. La Flota de Reservas de capacidad define los permisos de sus roles vinculados a servicios y, a menos que esté definido de otra manera, solo la Flota de Reservas de capacidad puede asumir sus roles. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM.

Solo es posible eliminar un rol vinculado a un servicio después de eliminar sus recursos relacionados. De esta forma, se protegen los recursos de la Flota de Reservas de capacidad, ya que se evita que se puedan eliminar accidentalmente permisos de acceso a los recursos.

Permisos de roles vinculados a servicios para la flota de reservas de capacidad

La Flota de Reservas de capacidad usa el rol vinculado a servicio denominado AWSServiceRoleForEC2CapacityReservationFleet para crear, describir, modificar y cancelar las Reservas de capacidad previamente creadas por una Flota de Reservas de capacidad, en su nombre.

El rol vinculado a servicio AWSServiceRoleForEC2CapacityReservationFleet confía en que la siguiente entidad asuma el rol: `capacity-reservation-fleet.amazonaws.com`.

El rol utiliza la política AWSEC2CapacityReservationFleetRolePolicy, que incluye los siguientes permisos:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeCapacityReservations",
                "ec2:DescribeInstances"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                "ec2:CreateCapacityReservation",
                "ec2:CancelCapacityReservation",
                "ec2:ModifyCapacityReservation"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:capacity-reservation/*"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:CapacityReservationFleet": "arn:aws:ec2:*:*:capacity-
reservation-fleet/crf-*"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:capacity-reservation/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateCapacityReservation"
                }
            }
        }
    ]
}
```

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Creación de un rol vinculado a servicios para la flota de reservas de capacidad

No necesita crear manualmente un rol vinculado a servicios. Al crear una Flota de Reservas de capacidad con el comando `create-capacity-reservation-fleet` de la AWS CLI o el comando de API `CreateCapacityReservationFleet`, el rol vinculado a servicio se crea automáticamente.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Al crear una Flota de Reservas de capacidad, la Flota de Reservas de capacidad crea de nuevo el rol vinculado a servicio.

Edición de un rol vinculado a servicios para la flota de reservas de capacidad

La Flota de Reservas de capacidad no le permite editar el rol vinculado a servicio AWSServiceRoleForEC2CapacityReservationFleet. Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminación de un rol vinculado a servicios para la flota de reservas de capacidad

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma no tiene una entidad no utilizada que no se monitoree ni mantenga de forma activa. No obstante, debe eliminar los recursos del rol vinculado a servicio antes de eliminarlo manualmente.

> **Note**
>
> Si el servicio de la Flota de Reservas de capacidad está utilizando el rol cuando intenta eliminar los recursos, la eliminación podría producir un error. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar el rol vinculado a servicio AWSServiceRoleForEC2CapacityReservationFleet

1. Utilice el comando `delete-capacity-reservation-fleet` de la AWS CLI o el comando de API `DeleteCapacityReservationFleet` para eliminar las flotas de Reservas de capacidad de su cuenta.
2. Utilice la consola de IAM, la AWS CLI o la API de AWS para eliminar el rol vinculado a servicio AWSServiceRoleForEC2CapacityReservationFleet. Para obtener más información, consulte Eliminar un rol vinculado a un servicio en la Guía del usuario de IAM.

Regiones admitidas para los roles vinculados a servicios de la flota de reservas de capacidad

La Flota de Reservas de capacidad admite el uso de roles vinculados a servicios en todas las regiones en las que el servicio esté disponible. Para obtener más información, consulte Puntos de conexión y regiones de AWS.

Reservas de capacidad de monitoreo

Puede utilizar las siguientes características para monitorear sus reservas de capacidad:

Temas

- Supervisión de las reservas de capacidad con las métricas de CloudWatch
- Supervisión de las reservas de capacidad mediante EventBridge
- Notificaciones de utilización

Supervisión de las reservas de capacidad con las métricas de CloudWatch

Con las métricas de CloudWatch, puede monitorear de forma eficiente las Reservas de capacidad e identificar la capacidad no utilizada configurando alarmas de CloudWatch que notifiquen cuándo se alcancen los umbrales de uso. Esto puede ayudarle a mantener un volumen de Reserva de capacidad constante y lograr un mayor nivel de utilización.

Reservas de capacidad bajo demanda envía datos de métricas a CloudWatch cada cinco minutos. Las métricas no se admiten para Reservas de capacidad que estén activas durante menos de cinco minutos.

Para obtener más información sobre cómo ver métricas en la consola de CloudWatch, consulte Uso de las métricas de Amazon CloudWatch. Para obtener más información acerca de la creación de alarmas, consulte Creación de alarmas de Amazon CloudWatch Alarms.

Contenido

- Métricas de uso de Reserva de capacidad
- Dimensiones de métricas de Reserva de capacidad
- Ver métricas de CloudWatch para Reservas de capacidad

Métricas de uso de Reserva de capacidad

El espacio de nombres `AWS/EC2CapacityReservations` incluye las siguientes métricas de uso que puede utilizar para monitorear y mantener la capacidad bajo demanda dentro de los umbrales especificados para su reserva.

Métrica	Descripción
`UsedInstanceCount`	El número de instancias que se están utilizando actualmente. Unidad: recuento
`AvailableInstanceCount`	El número de instancias que están disponibles. Unidad: recuento
`TotalInstanceCount`	El número total de instancias que ha reservado. Unidad: recuento
`InstanceUtilization`	El porcentaje de instancias de capacidad reservadas que se están utilizando actualmente. Unidad: porcentaje

Dimensiones de métricas de Reserva de capacidad

Puede utilizar las siguientes dimensiones para ajustar las métricas mostradas en la tabla anterior.

Dimensión	Descripción
`CapacityReservationId`	Esta dimensión única global filtra los datos que solicita solo para la reserva de capacidad identificada.

Ver métricas de CloudWatch para Reservas de capacidad

Las métricas se agrupan en primer lugar por el espacio de nombres de servicio y, a continuación, por las dimensiones compatibles. Puede usar los siguientes procedimientos para ver las métricas de Reservas de capacidad.

Para consultar las métricas de Reserva de capacidad con la consola de CloudWatch

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. Si es necesario, cambie la región. En la barra de navegación, seleccione la región donde reside la Reserva de capacidad. Para obtener más información, consulte Puntos de conexión y regiones.
3. En el panel de navegación, seleccione Metrics (Métricas).
4. En Todas las métricas, elija Reservas de capacidad de EC2.
5. Elija la dimensión métrica Por reserva de capacidad. Las métricas se agruparán por `CapacityReservationId`.
6. Para ordenar las métricas, utilice el encabezado de columna. Para representar gráficamente una métrica, active la casilla de verificación situada junto a ella.

Para ver las métricas de la reserva de capacidad (AWS CLI)

Utilice el siguiente comando list-metrics:

```
aws cloudwatch list-metrics --namespace "AWS/EC2CapacityReservations"
```

Supervisión de las reservas de capacidad mediante EventBridge

AWS Health envía eventos a Amazon EventBridge cuando una reserva de capacidad en su cuenta está por debajo del 20 por ciento de uso durante ciertos periodos. Con EventBridge, puede establecer reglas que activen acciones programáticas en respuesta a dichos eventos. Por ejemplo, puede crear una regla que cancele automáticamente una reserva de capacidad cuando su utilización caiga por debajo del 20 por ciento de utilización en un periodo de 7 días.

Los eventos en EventBridge se representan como objetos JSON. Los campos que son únicos del evento se encuentran en la sección "detail" del objeto JSON. El campo “evento” contiene el nombre del evento. El campo “resultado” contiene el estado completad de la acción que desencadenó el evento. Para obtener más información, consulte Amazon EventBridge event patterns (Patrones de eventos de Amazon EventBridge) en la Guía del usuario de Amazon EventBridge.

Para más información, consulte la Guía del usuario de Amazon EventBridge.

Esta característica no es compatible con AWS GovCloud (US).

Contenido

Eventos

AWS Health envía los siguientes eventos cuando el uso de la capacidad de una reserva de capacidad es inferior al 20 por ciento.

Eventos

- AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION
- AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY

AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION

El siguiente es un ejemplo de un evento que se genera cuando una reserva de capacidad recién creada tiene un uso de capacidad inferior al 20 por ciento durante un periodo de 24 horas.

```
{
    "version": "0",
    "id": "b3e00086-f271-12a1-a36c-55e8ddaa130a",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2023-03-10T12:03:38Z",
    "region": "ap-south-1",
    "resources": [
        "cr-01234567890abcdef"
    ],
    "detail": {
        "eventArn": "arn:aws:health:ap-south-1::event/EC2/
AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION/
AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_cr-01234567890abcdef-6211-4d50-9286-0c9fbc243f04",
        "service": "EC2",
        "eventTypeCode": "AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION",
        "eventTypeCategory": "accountNotification",
```

```
        "startTime": "Fri, 10 Mar 2023 12:03:38 GMT",
        "endTime": "Fri, 10 Mar 2023 12:03:38 GMT",
        "eventDescription": [
            {
                "language": "en_US",
                "latestDescription": "A description of the event will be provided here"
            }
        ],
        "affectedEntities": [
            {
                "entityValue": "cr-01234567890abcdef"
            }
        ]
    }
    }
```

AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY

El siguiente es un ejemplo de un evento que se genera cuando una o más reservas de capacidad tienen un uso de capacidad inferior al 20 por ciento durante un periodo de 7 días.

```
{
    "version": "0", "id":"7439d42b-3c7f-ad50-6a88-25e2a70977e2",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2023-03-07T06:06:01Z",
    "region": "us-east-1",
    "resources": [
        "cr-01234567890abcdef | us-east-1b | t3.medium | Linux/UNIX | 0.0%",
        "cr-09876543210fedcba | us-east-1a | t3.medium | Linux/UNIX | 0.0%"
    ],
    "detail": {
        "eventArn": "arn:aws:health:us-east-1::event/EC2/
AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY/
AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY_726c1732-d6f6-4037-b9b8-
bec3c2d3ba65",
        "service": "EC2",
        "eventTypeCode": "AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY",
        "eventTypeCategory": "accountNotification",
        "startTime": "Tue, 7 Mar 2023 06:06:01 GMT",
        "endTime": "Tue, 7 Mar 2023 06:06:01 GMT",
        "eventDescription": [
```

```
            {
                "language": "en_US",
                "latestDescription": "A description of the event will be provided
 here"
            }
        ],
        "affectedEntities": [
            {
                "entityValue": "cr-01234567890abcdef | us-east-1b | t3.medium | Linux/
UNIX | 0.0%"
            },
            {
                "entityValue": "cr-09876543210fedcba | us-east-1a | t3.medium | Linux/
UNIX | 0.0%"
            }
        ]
    }
}
```

Crear una regla de EventBridge

Para recibir notificaciones por correo electrónico cuando el uso de reserva de capacidad sea inferior al 20 por ciento, cree un tema de Amazon SNS y, luego, cree una regla de Amazon SNS y una regla de EventBridge para el evento `AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION`.

Para crear el tema de Amazon SNS

1. Abra la consola de Amazon SNS en https://console.aws.amazon.com/sns/v3/home.
2. En el panel de navegación, elija Temas y, a continuación, seleccione Crear tema.
3. En Tipo, seleccione Estándar.
4. En Nombre, escriba un nombre para el nuevo tema.
5. Elija Crear nuevo tema.
6. Elija Crear una suscripción.
7. En Protocolo, elija Correo electrónico y, a continuación, en Punto de conexión, introduzca la dirección de correo electrónico que recibe las notificaciones.
8. Seleccione Crear una suscripción.
9. La dirección de correo electrónico ingresada anteriormente recibirá un mensaje de correo electrónico con la siguiente línea de asunto: `AWS Notification - Subscription Confirmation`. Siga las instrucciones para confirmar la suscripción.

Para crear la regla de EventBridge

1. Abra la consola de Amazon EventBridge en https://console.aws.amazon.com/events/.
2. En el panel de navegación, elija Rules (Reglas) y, a continuación, elija Create rule (Crear regla).
3. En Nombre, ingrese el nombre de la nueva regla.
4. En Tipo de regla, elija Regla con un patrón de evento.
5. Elija Siguiente.
6. En Patrón de evento, realice lo siguiente:
    a. En Origen de evento, seleccione Servicios de AWS.
    b. En Servicio de AWS, seleccione AWS Health.
    c. Para el Tipo de evento, elija Notificación de poca utilización de ODCR de EC2.
7. Elija Siguiente.
8. En Destinos 1, haga lo siguiente:
    a. En Tipos de destino, seleccione Servicio de AWS.
    b. Para Seleccione un destino, elija Tema de SNS.
    c. En Tema, elija el tema que creó anteriormente.
9. Elija Siguiente y después elija de nuevo Siguiente.
10. Elija Crear regla.

Notificaciones de utilización

AWS Health envía el siguiente correo electrónico y las notificaciones AWS Health Dashboardcuando la utilización de la capacidad de reservas de capacidad de su cuenta caiga por debajo del 20 por ciento.

- Notificaciones individuales para cada reserva de capacidad recién creada que haya estado por debajo del 20 por ciento de utilización durante las últimas 24 horas.
- Una notificación resumida para todas las reservas de capacidad que hayan estado por debajo del 20 por ciento de utilización durante los últimos 7 días.

Las notificaciones de correo electrónico y las notificaciones AWS Health Dashboard se envían a la dirección de correo electrónico asociada a la cuenta de AWS que es propietaria de las reservas de capacidad. Las notificaciones incluyen la siguiente información:

- El ID de la reserva de capacidad.
- La zona de disponibilidad de la reserva de capacidad.
- La tasa de utilización promedio de la reserva de capacidad.
- El tipo de instancia y la plataforma (sistema operativo) de la reserva de capacidad.

Además, cuando el uso de la capacidad de una reserva de capacidad en su cuenta cae por debajo del 20 por ciento en un periodo de 24 y 7 días, AWS Health envía los eventos a EventBridge. Con EventBridge, puede crear reglas que activen las acciones automáticas, como el envío de notificaciones por correo electrónico o la activación de funciones de AWS Lambda, en respuesta a dichos eventos. Para obtener más información, consulte Supervisión de las reservas de capacidad mediante EventBridge.

bloques de capacidad para ML

bloques de capacidad para ML le permite reservar instancias de GPU que tienen una alta demanda para el futuro a fin de respaldar sus cargas de trabajo de machine learning (ML) de corta duración. Las instancias que se ejecutan en un bloque de capacidad se colocan automáticamente juntas dentro de ultraclústeres de Amazon EC2 para conseguir redes que no generen bloqueos, de escala de petabits y de baja latencia.

Con bloques de capacidad, puede ver cuándo estará disponible la capacidad de las instancias de GPU en fechas futuras y programar un bloque de capacidad para que comience a la hora que mejor le convenga. Cuando reserva un bloque de capacidad, obtiene una garantía de capacidad predecible para las instancias de GPU y paga solo por el tiempo que necesite. Recomendamos bloques de capacidad si necesita GPU para respaldar sus cargas de trabajo de ML durante días o semanas y no quiere pagar una reserva mientras las instancias de GPU no estén en uso.

A continuación, se indican algunos casos de uso frecuentes de bloques de capacidad.

- Entrenamiento y ajuste de modelos de ML: obtenga acceso ininterrumpido a las instancias de GPU que reservó para completar el entrenamiento y el ajuste de los modelos de ML.
- Experimentos y prototipos de ML: ejecute experimentos y cree prototipos que requieran instancias de GPU durante periodos cortos.

Los bloques de capacidad están disponibles actualmente para instancias `p5.48xlarge` y `p4d.24xlarge`. Las instancias `p5.48xlarge` están disponibles en las regiones Este de EE. UU. (Ohio) y Este de EE. UU. (Norte de Virginia). Las instancias `p4d.24xlarge` están disponibles en

las regiones Este de EE. UU. (Ohio) y Oeste de EE. UU. (Oregón). Puede reservar un bloque de capacidad con una hora de inicio de reserva de hasta ocho semanas en el futuro.

Puede usar bloques de capacidad para reservar instancias p5 y p4d con las siguientes opciones de duración de reserva y cantidad de instancias.

- La duración de las reservas de 1 día se incrementa hasta un total de 14 días
- Opciones de cantidad de instancias de reserva de 1, 2, 4, 8, 16, 32 o 64 instancias

Para reservar un bloque de capacidad, comience por especificar sus necesidades de capacidad, lo que incluye, el tipo de instancias, la cantidad de instancias, la cantidad de tiempo, la fecha de inicio más temprana y la fecha de finalización más tardía que necesita. A continuación, podrá ver una oferta de bloques de capacidad disponible que cumpla con sus especificaciones. La oferta de bloques de capacidad incluye detalles como la hora de inicio, la zona de disponibilidad y el precio de la reserva. El precio de una oferta de bloques de capacidad depende de la oferta y la demanda disponibles en el momento en que se hizo la oferta. Después de reservar un bloque de capacidad, el precio no cambia. Para obtener más información, consulte Precios y facturación de bloques de capacidad.

Al comprar una oferta de bloques de capacidad, la reserva se crea para la fecha y el número de instancias que haya seleccionado. Cuando comience su reserva de bloques de capacidad, podrá especificar el ID de reserva en sus solicitudes de inicialización para segmentar los inicializacións de instancias.

Puede usar todas las instancias que reservó hasta 30 minutos antes de la hora de finalización del bloque de capacidad. Cuando queden 30 minutos de su reserva de bloques de capacidad, comenzaremos a terminar todas las instancias que se estén ejecutando en el bloque de capacidad. Aprovechamos este tiempo para limpiar sus instancias antes de entregar el bloque de capacidad al siguiente cliente. Los últimos 30 minutos de la reserva no se incluyen en el precio del bloque de capacidad. Emitimos un evento a través de EventBridge 10 minutos antes de que comience el proceso de terminación. Para obtener más información, consulte Supervisión de los bloques de capacidad con EventBridge.

Temas

- Precios y facturación de bloques de capacidad
- Uso de bloques de capacidad
- Supervisión de los bloques de capacidad

Plataformas admitidas

Los bloques de capacidad para ML admiten actualmente instancias `p5.48xlarge` y `p4d.24xlarge` con una tenencia predeterminada. Cuando se utiliza AWS Management Console para comprar un bloque de capacidad, la opción de plataforma predeterminada es Linux/UNIX. Al usar la AWS Command Line Interface (AWS CLI) o el SDK de AWS al comprar un bloque de capacidad, están disponibles las siguientes opciones de plataforma:

- Linux/Unix
- Red Hat Enterprise Linux
- RHEL con HA
- SUSE Linux
- Ubuntu Pro

Consideraciones

Antes de usar los bloques de capacidad, tenga en cuenta los siguientes detalles y limitaciones.

- Los bloques de capacidad comienzan y terminan a las 11:30 h UTC (horario universal coordinado).
- El proceso de terminación de las instancias que se ejecutan en un bloque de capacidad comienza a las 11:00 h UTC (horario universal coordinado) el último día de la reserva.
- Los bloques de capacidad se pueden reservar con una hora de inicio con hasta 8 semanas de antelación.
- No se admiten modificaciones ni cancelaciones de los bloques de capacidad.
- Los bloques de capacidad no se pueden compartir entre cuentas de AWS ni dentro de su organización de AWS.
- Los bloques de capacidad no se pueden usar en un grupo de reserva de capacidad.
- El número total de instancias que se pueden reservar en bloques de capacidad en todas las cuentas de su organización de AWS no puede superar las 64 instancias en una fecha determinada.
- Para usar un bloque de capacidad, las instancias deben dirigirse específicamente al ID de reserva.

- Las instancias de un bloque de capacidad no se tienen en cuenta para los límites de instancias bajo demanda.
- En el caso de las instancias P5 que utilizan una AMI personalizada, asegúrese de tener el software y la configuración necesarios para la EFA.
- Los bloques de capacidad actualmente no se pueden usar con grupos de nodos administrados por Amazon EKS o Karpenter. Para obtener más información sobre cómo crear un grupo de nodos autogestionado de Amazon EKS, consulte Bloques de capacidad para ML en la Guía del usuario de Amazon EKS.

Recursos relacionados

Después de crear un bloque de capacidad, podrá hacer lo siguiente con el bloque de capacidad:

- inicialización de instancias en el bloque de capacidad Para obtener más información, consulte inicialización de instancias en bloques de capacidad.
- Crear un grupo de Amazon EC2 Auto Scaling. Para obtener más información, consulte Use Capacity Blocks for machine learning workloads en la Guía del usuario de Amazon EC2 Auto Scaling.

  > **Note**
  >
  > Si utiliza Amazon EC2 Auto Scaling o Amazon EKS, puede programar el escalado para que se ejecute al inicio de la reserva del bloque de capacidad. Con el escalado programado, AWS administra automáticamente los reintentos, por lo que no tiene que preocuparse por implementar una lógica de reintentos para administrar los errores transitorios.

- Mejore los flujos de trabajo de ML con AWS ParallelCluster. Para obtener más información, consulte Mejora de los flujos de trabajo de ML con AWS ParallelCluster y los bloques de capacidad de Amazon EC2 para ML.

Para obtener más información acerca de AWS ParallelCluster, consulte ¿Qué es AWS ParallelCluster?.

Precios y facturación de bloques de capacidad

Temas

- Precios
- Facturación

Precios

Con bloques de capacidad para ML de Amazon EC2, paga únicamente por lo que reserva. El precio de un bloque de capacidad depende de la oferta y la demanda de bloques de capacidad disponibles en el momento de la compra. Puede consultar el precio de una oferta de bloques de capacidad antes de reservarla. El precio del bloque de capacidad se cobra por adelantado en el momento de realizar la reserva. Si busca un bloque de capacidad en un rango de fechas, le mostramos la oferta de bloques de capacidad con el precio más bajo disponible. Después de haber reservado un bloque de capacidad, el precio no cambia.

Cuando utiliza un bloque de capacidad, paga por el sistema operativo que utiliza cuando las instancias están en ejecución. Para obtener más información acerca de los precios, consulte Precios de los Bloques de capacidad de Amazon EC2 para ML.

Facturación

El precio de una oferta de bloques de capacidad se cobra por adelantado. El pago se facturará a su cuenta de AWS 12 horas después de la compra de un bloque de capacidad. Mientras se procesa el pago, su recurso de reserva de bloques de capacidad permanece en el estado `payment-pending`. Si el pago no se puede procesar en un plazo de 12 horas, se liberará el bloque de capacidad y el estado de la reserva cambiará a `payment-failed`.

Una vez que el pago se haya procesado correctamente, el estado del recurso de bloques de capacidad cambiará de `payment-pending` a `scheduled`. Recibirá una factura en la que se reflejará el pago inicial único. En la factura, puede asociar el importe pagado al ID de reserva de bloques de capacidad.

Cuando comience su reserva de bloques de capacidad, se le facturará únicamente en función del sistema operativo que utilice mientras las instancias estén activas en la reserva. Puede ver su uso y los cargos asociados en su factura de aniversario correspondiente al mes de uso en su AWS Cost and Usage Report.

> **Note**
>
> Los descuentos de Savings Plans e instancias reservadas no se aplican a bloques de capacidad.

Visualización de su factura

Puede ver su factura en la consola de AWS Billing and Cost Management. El pago inicial de su bloque de capacidad aparece en el mes en que compró la reserva.

Una vez iniciada la reserva, en la factura se muestran líneas separadas para el tiempo que se ha utilizado y que no se ha utilizado la reserva de bloques. Puede usar estas líneas para ver cuánto tiempo se utilizó en su reserva. Si utiliza un sistema operativo premium, solo verá un cargo por uso en la línea del tiempo utilizado. Para obtener más información, consulte Precios. No hay cargos adicionales por el tiempo no utilizado.

Para obtener más información, consulte Ver su factura en la Guía del usuario de AWS Billing and Cost Management.

Si el bloque de capacidad comienza en un mes diferente al mes en que compró la reserva, el precio inicial y el uso de la reserva se muestran en meses de facturación distintos. En su AWS Cost and Usage Report, el ID de reserva de bloques de capacidad aparece en la línea Reservation/ReservationARN de su tarifa inicial y en lineitem/ResourceID de su factura de aniversario para que pueda asociar el uso al precio inicial correspondiente.

Uso de bloques de capacidad

Para empezar a usar bloques de capacidad, primero debe buscar y comprar un bloque de capacidad disponible que se adapte al tamaño, la duración y el tiempo de su reserva. Luego, cuando comience la reserva, puede usar el bloque de capacidad al iniciar instancias que se dirijan al ID de reserva. Treinta minutos antes de que caduque la reserva, empezaremos a terminar todas las instancias que aún estén en ejecución en el bloque de capacidad.

Los bloques de capacidad se entregan como reservas de capacidad `targeted` en una única zona de disponibilidad. Para ejecutar instancias en un bloque de capacidad, debe especificar el ID de reserva al iniciar las instancias. Si detiene las instancias por su cuenta y el bloque de capacidad vence, no podrá reanudarlas hasta que se dirija a otro bloque de capacidad que tenga el estado `active`.

De forma predeterminada, bloques de capacidad ofrece conectividad de red de baja latencia y alto rendimiento entre las instancias incluidas en el bloque de capacidad, por lo que no es necesario utilizar un grupo con ubicación en clúster con un bloque de capacidad.

Temas

Requisitos previos

Debe utilizar la Región de AWS correspondiente para el tipo de instancias que desea utilizar. Para obtener más información, consulte Regiones.

Los bloques de capacidad con instancias `p5.48xlarge` están disponibles en las siguientes Regiones de AWS.

Nombre de la región	Código de región
Este de EE. UU. (Ohio)	us-east-2
Este de EE. UU. (Norte de Virginia)	us-east-1

Los bloques de capacidad con instancias `p4d.24xlarge` están disponibles en las siguientes Regiones de AWS.

Nombre de la región	Código de región
Este de EE. UU. (Ohio)	us-east-2
Oeste de EE. UU. (Oregón)	us-west-2

> **Note**
>
> No todos los tipos de instancias de todas las Regiones de AWS admiten tamaños de bloques de capacidad de 64 instancias.

Búsqueda y compra de bloques de capacidad

Para reservar un bloque de capacidad, primero tiene que encontrar un bloque de tiempo en el que haya capacidad disponible que se adapte a sus necesidades. Para encontrar un bloque de capacidad que se pueda reservar, debe especificar:

- El número de instancias que necesita
- El tiempo durante el que necesita las instancias
- El intervalo de fechas en el que necesita su reserva

Para buscar una oferta de bloques de capacidad disponible, especifique la duración de la reserva y el número de instancias. Debe seleccionar una de las siguientes opciones.

- Para la duración de la reserva: hasta 14 días en incrementos de 1 día
- Para el recuento de instancias: 1, 2, 4, 8, 16, 32 o 64 instancias

Si hay un bloque de capacidad disponible que se ajuste a sus especificaciones, le devolveremos los detalles de una única oferta de bloques de capacidad. Los detalles de la oferta incluyen la hora de inicio de la reserva, la zona de disponibilidad de la reserva y el precio de la reserva. Para obtener más información, consulte Precios.

Puede comprar la oferta de bloques de capacidad que se muestra o puede modificar sus criterios de búsqueda para ver las demás opciones disponibles. No hay una fecha de caducidad predefinida para la oferta, pero las ofertas solo están disponibles por orden de llegada.

Cuando compra una oferta de bloques de capacidad, recibe una respuesta inmediata que confirma que su bloque de capacidad está reservado. Tras la confirmación, verá una nueva reserva de capacidad en su cuenta con el tipo de reserva `capacity-block` y el valor de `start-date` establecido en la hora de inicio de la oferta que ha adquirido. Su reserva de bloques de capacidad se crea con un estado de `payment-pending`. Una vez que el pago inicial se haya procesado correctamente, el estado de la reserva cambiará a `scheduled`. Para obtener más información, consulte Facturación.

Puede utilizar uno de los métodos siguientes para buscar y comprar un bloque de capacidad.

Console

Búsqueda y compra de un bloque de capacidad mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la barra de navegación de la parte superior de la pantalla, debe seleccionar una Región de AWS. Esta elección es importante porque no todos los tipos de instancias de todas las regiones admiten tamaños de bloques de capacidad de 64 instancias.
3. En el panel de navegación, seleccione Reservas de capacidad y Comprar bloques de capacidad.
4. En Atributos de capacidad, puede definir los parámetros de búsqueda del bloque de capacidad. De forma predeterminada, la plataforma es Linux. Si quiere seleccionar un sistema operativo diferente, use AWS CLI. Para obtener más información, consulte Plataformas admitidas.
5. En Capacidad total, seleccione el número de instancias que desea reservar.
6. En Duración, ingrese el número de días para los que necesita la reserva.
7. En Intervalo de fechas para buscar bloques de capacidad, ingrese la fecha de inicio más temprana posible y la última fecha de finalización aceptable para su reserva.
8. Elija Buscar bloques de capacidad.
9. Si hay un bloque de capacidad disponible que cumpla sus especificaciones, verá una oferta en bloques de capacidad recomendados. Si hay varias ofertas que cumplen sus especificaciones, se muestra la oferta de bloques de capacidad con el precio más bajo disponible. Para ver otras ofertas de bloques de capacidad, ajuste las entradas de búsqueda y vuelva a seleccionar Buscar bloques de capacidad.
10. Cuando encuentre una oferta de bloques de capacidad que desee comprar, seleccione Siguiente.
11. (Opcional) En la página Agregar etiquetas, elija Agregar nueva etiqueta.
12. En la página Revisar y comprar se muestran la fecha de inicio y finalización, la duración, el número total de instancias y el precio.

> **Note**
>
> Los bloques de capacidad no se pueden modificar ni cancelar una vez que los haya reservado.

13. En la ventana emergente Comprar un bloque de capacidad, escriba confirmar y, a continuación, seleccione Comprar.

AWS CLI

Búsqueda de un bloque de capacidad mediante la AWS CLI

Utilice el comando `describe-capacity-block-offerings`.

En el siguiente ejemplo, se busca un bloque de capacidad que tenga 16 instancias `p5.48xlarge` con un intervalo de fechas entre `2023-08-14` y `2023-10-22` y que tenga una duración de 48 horas. El recuento de instancias debe ser un número entero de un conjunto predefinido de opciones 1, 2, 4, 8, 16, 32, 64. La duración de la capacidad debe ser un número entero que sea un múltiplo de 24, entre 24 y 336, lo que indica el número de días en horas.

```
aws ec2 describe-capacity-block-offerings --instance-type p5.48xlarge \
  --instance-count 16 --start-date-range 2023-08-14T00:00:00Z \
  --end-date-range 2023-10-22-T00:00:00Z --capacity-duration 48
```

Compra de un bloque de capacidad mediante la AWS CLI

Utilice el comando `purchase-capacity-block` y especifique el ID de oferta del bloque de capacidad que desee comprar y la plataforma de instancias.

```
aws ec2 purchase-capacity-block \
  --capacity-block-offering-id cbr-0123456789abcdefg \
  --instance-platform Linux/UNIX
```

inicialización de instancias en bloques de capacidad

Después de reservar un bloque de capacidad, podrá ver la reserva de bloques de capacidad en su cuenta de AWS. Puede consultar los valores `start-date` y `end-date` para ver cuándo comenzará y finalizará su reserva. Antes de que comience una reserva de bloques de capacidad, la capacidad disponible aparece como cero. Puede ver cuántas instancias estarán disponibles en su bloque de capacidad mediante el valor de etiqueta de la clave de etiqueta `aws:ec2capacityreservation:incrementalRequestedQuantity`.

Cuando comienza una reserva de bloque de capacidad, el estado de la reserva cambia de `scheduled` a `active`. Emitimos un evento a través de Amazon EventBridge para notificarle

que el bloque de capacidad está disponible para usarse. Para obtener más información, consulte Supervisión de los bloques de capacidad.

Para usar su bloque de capacidad, debe especificar el ID de reserva del bloque de capacidad al iniciar las instancias. la inicialización de una instancia en un bloque de capacidad reduce la capacidad disponible por número de instancias iniciadas. Por ejemplo, si la capacidad de instancias comprada es de ocho instancias y inicia cuatro instancias, la capacidad disponible se reduce en cuatro.

Si termina una instancia que se está ejecutando en el bloque de capacidad antes de que finalice la reserva, puede iniciar una nueva instancia en su lugar. Cuando detiene o termina una instancia en un bloque de capacidad, se necesitan varios minutos para limpiar la instancia antes de poder iniciar otra instancia para reemplazarla. Durante este tiempo, la instancia estará en estado de detención o `shutting-down`. Una vez finalizado este proceso, el estado de la instancia cambiará a `stopped` o `terminated`. A continuación, la capacidad disponible en su bloque de capacidad se actualizará para mostrar otra instancia disponible para usarse.

En los siguientes pasos se explica cómo iniciar instancias en un bloque de capacidad en estado `active` mediante la AWS Management Console o AWS CLI.

Para obtener información sobre cómo configurar un grupo de nodos de EKS para que utilice automáticamente un bloque de capacidad cuando comience, consulte bloques de capacidad para ML en la Guía del usuario de Amazon EKS.

Para obtener información sobre cómo iniciar instancias en un bloque de capacidad mediante flota de EC2, consulte Tutorial: Inicialización de instancias en bloques de capacidad.

Para obtener información sobre cómo crear una plantilla de inicialización dirigida a un bloque de capacidad, consulte iniciar una instancia desde una plantilla de inicialización.

Puede utilizar uno de los métodos siguientes para iniciar instancias en un bloque de capacidad.

Console

inicialización de instancias en un bloque de capacidad con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la barra de navegación de la parte superior de la pantalla, seleccione la región para la reserva de bloques de capacidad.
3. En el panel de la consola de Amazon EC2, elija iniciar instancia.

4. (Opcional) En Nombre y etiquetas, puede asignar un nombre a su instancia y etiquetarla. Para obtener más información acerca de las etiquetas, consulte Etiquetar los recursos de Amazon EC2
5. En Imágenes de aplicaciones y sistema operativo, seleccione una Imagen de máquina de Amazon (AMI).
6. En Tipo de instancia, seleccione el tipo de instancia que coincida con su reserva de bloques de capacidad.
7. En Par de claves (inicio de sesión), elija un par de claves existente o elija Crear un par de claves nuevo para crear uno nuevo. Para obtener más información, consulte Pares de claves e instancias de Amazon EC2.
8. En Network settings (Configuración de red), utilice la configuración predeterminada o elija Edit (Editar) para configurar los ajustes de red según sea necesario.

   > **Important**
   >
   > La instancia no se puede iniciar en una subred de una zona de disponibilidad diferente a la zona de disponibilidad en la que se encuentra el bloque de capacidad.

9. En Detalles avanzados, configure la instancia de la siguiente manera.
   a. En la Opción de compra (tipo de mercado), seleccione bloques de capacidad.
   b. En Reserva de capacidad, seleccione Destino por ID.
   c. Seleccione el ID de reserva de capacidad de su reserva de bloques de capacidad.
10. En el panel Resumen, en Cantidad de instancias, escriba la cantidad de instancias que iniciará.
11. Seleccione iniciar instancia.

AWS CLI

inicialización de instancias en un bloque de capacidad con la AWS CLI

- Utilice el comando `run-instances` y especifique el valor `capacity-block` en `MarketType` en la estructura de `instance-market-options`. También debe especificar el parámetro `capacity-reservation-specification`.

En el siguiente ejemplo se inicia una única instancia `p5.48xlarge` en cualquier bloque de capacidad activo que cuente con atributos coincidentes y capacidad disponible.

```
aws ec2 run-instances --image-id ami-abc12345 --count 1 \
  --instance-type p5.48xlarge --key-name MyKeyPair \
  --subnet-id subnet-1234567890abcdef1 \
  --instance-market-options MarketType='capacity-block'
  --capacity-reservation-specification
 CapacityReservationTarget={CapacityReservationId=cr-a1234567}
```

Visualización de bloques de capacidad

Los bloques de capacidad tienen los siguientes estados:

- `payment-pending`: el pago inicial aún no se ha procesado.
- `payment-failed`: el pago no se pudo procesar en el plazo de 12 horas. Se ha liberado su bloque de capacidad.
- `scheduled`: el pago se procesó y la reserva de bloques de capacidad aún no ha comenzado.
- `active`: la capacidad reservada está disponible para su uso.
- `expired`: la reserva de bloques de capacidad caducó automáticamente en la hora y fecha especificadas en su solicitud de reserva. La capacidad reservada ya no está disponible para su uso.

Puede utilizar uno de los métodos siguientes para ver la reserva de bloques de capacidad.

Console

Visualización de bloques de capacidad con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Reservas de capacidad.
3. En la página Información general sobre las reservas de capacidad, verá una tabla de recursos con detalles sobre todos sus recursos de reservas de capacidad. Para encontrar sus reservas de bloques de capacidad, seleccione bloques de capacidad en la lista desplegable situada encima de ID de reserva de capacidad. En la tabla, puede ver

información sobre sus bloques de capacidad, como las fechas de inicio y finalización, la duración y el estado.

4. Para obtener más información sobre un bloque de capacidad, seleccione el ID de reserva del bloque de capacidad que desee ver. En la página Detalles de la reserva de capacidad se muestran todas las propiedades de la reserva y el número de instancias en uso y disponibles en el bloque de capacidad.

> **Note**
>
> Antes de que comience una reserva de bloques de capacidad, la capacidad disponible aparece como cero. Puede ver cuántas instancias estarán disponibles cuando la reserva del bloque de capacidad comience con el siguiente valor de etiqueta para la clave de etiqueta: `aws:ec2capacityreservation:incrementalRequestedQuantity`.

AWS CLI

Visualización de bloques de capacidad con la AWS CLI

De forma predeterminada, cuando se utiliza el comando describe-capacity reservations, aparecen tanto las reserva de capacidad bajo demanda como las reservas de bloques de capacidad. Para ver solo las reservas de bloques de capacidad, filtre con `capacity-block` según el parámetro `capacity-reservation-type`.

Por ejemplo, el siguiente comando describe una o varias de las reservas de bloques de capacidad en la Región de AWS actual.

```
aws ec2 describe-capacity-reservations -reservation-type capacity-block
```

Resultado de ejemplo.

```
{
    "CapacityReservations": [
        {
            "CapacityReservationId": "cr-12345678",
            "EndDateType": "limited",
            "ReservationType": "capacity-block"
            "AvailabilityZone": "eu-east-2a",
            "InstanceMatchCriteria": "targeted",
```

```
            "EphemeralStorage": false,
            "CreateDate": "2023-11-29T14:22:45Z",
            "StartDate": "2023-12-15T12:00:00Z",
            "EndDate": "2023-08-19T12:00:00Z",
            "AvailableInstanceCount": 0,
            "InstancePlatform": "Linux/UNIX",
            "TotalInstanceCount": 16,
            "State": "payment-pending",
            "Tenancy": "default",
            "EbsOptimized": true,
            "InstanceType": "p5.48xlarge"
        },
        ...
```

Supervisión de los bloques de capacidad

Temas

- Supervisión de los bloques de capacidad con EventBridge
- Registro de llamadas a la API de bloques de capacidad con AWS CloudTrail

Supervisión de los bloques de capacidad con EventBridge

Cuando comience su reserva de bloques de capacidad, Amazon EC2 emitirá un evento a través de EventBridge que indicará que su capacidad está lista para usarse. Cuarenta minutos antes de que finalice la reserva de bloques de capacidad, recibirá otro evento de EventBridge en el que se le indicará que cualquier instancia que se esté ejecutando en la reserva empezará a terminarse en 10 minutos. Para más información acerca de los eventos de EventBridge, consulte Eventos de Amazon EventBridge.

Las siguientes estructuras de eventos para los eventos emitidos para bloques de capacidad:

bloque de capacidad entregado

En el ejemplo siguiente se muestra un evento de un bloque de capacidad entregado.

```
{
  "customer_event_id": "[Capacity Reservation Id]-delivered",
  "detail_type": "Capacity Block Reservation Delivered",
  "source": "aws.ec2",
  "account": "[Customer Account ID]",
```

```
  "time": "[Current time]",
  "resources": [
    "[ODCR ARN]"
  ],
  "detail": {
    "capacity-reservation-id": "[ODCR ID]",
    "end-date": "[ODCR End Date]"
  }
}
```

Advertencia de caducidad del bloque de capacidad

En el ejemplo siguiente se muestra un evento de advertencia de caducidad del bloque de capacidad.

```
{
  "customer_event_id": "[Capacity Reservation Id]-approaching-expiry",
  "detail_type": "Capacity Block Reservation Expiration Warning",
  "source": "aws.ec2",
  "account": "[Customer Account ID]",
  "time": "[Current time]",
  "resources": [
    "[ODCR ARN]"
  ],
  "detail": {
    "capacity-reservation-id": "[ODCR ID]",
    "end-date": "[ODCR End Date]"
  }
}
```

Registro de llamadas a la API de bloques de capacidad con AWS CloudTrail

bloques de capacidad se integra a AWS CloudTrail, un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un servicio de AWS en bloques de capacidad. CloudTrail captura las llamadas a la API de bloques de capacidad como eventos. Las llamadas capturadas incluyen las llamadas desde la consola de bloques de capacidad y las llamadas desde el código a las operaciones de la API de bloques de capacidad. Si crea un registro de seguimiento, puede habilitar la entrega continua de eventos de CloudTrail a un bucket de Amazon S3, incluidos los eventos de bloques de capacidad. Si no configura un registro de seguimiento, puede ver los eventos más recientes en la consola de CloudTrail en el Historial de eventos. Mediante la información que recopila CloudTrail, puede determinar la solicitud que se hizo a bloques de capacidad, la dirección IP desde la que se hizo dicha solicitud, quién la hizo y cuándo, además de información adicional.

Para más información sobre CloudTrail, consulte la Guía del usuario de AWS CloudTrail.

Información de bloques de capacidad en CloudTrail

CloudTrail se habilita en su Cuenta de AWS cuando se crea la cuenta. Cuando se produce una actividad en bloques de capacidad, esa actividad se registra en un evento de CloudTrail junto con otros eventos de servicios de AWS en Historial de eventos. Puede ver, buscar y descargar eventos recientes en su Cuenta de AWS. Para más información, consulte Visualización de eventos con el historial de eventos de CloudTrail.

Para mantener un registro continuo de los eventos en la Cuenta de AWS, incluidos los eventos de bloques de capacidad, cree un registro de seguimiento. Un registro de seguimiento permite a CloudTrail enviar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las Regiones de AWS. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. También es posible configurar otros servicios de AWS para analizar en profundidad y actuar en función de los datos de eventos recopilados en los registros de CloudTrail. Para más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- Servicios e integraciones compatibles con CloudTrail
- Configuración de notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de registro de CloudTrail de varias regiones y Recibir archivos de registro de CloudTrail de varias cuentas

Todas las acciones de bloques de capacidad las registra CloudTrail y se documentan en la Referencia de la API de Amazon EC2. Por ejemplo, las llamadas a las acciones `CapacityBlockScheduled` y `CapacityBlockActive` generan entradas en los archivos de registros de CloudTrail.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario lo ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario de AWS Identity and Access Management (IAM) o credenciales de usuario raíz.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.

- Si la solicitud la realizó otro servicio de AWS.

Para más información, consulte Elemento userIdentity de CloudTrail.

Descripción de las entradas de archivos de registro de bloques de capacidad

Un registro de seguimiento es una configuración que permite la entrega de eventos como archivos de registros en un bucket de Amazon S3 que especifique. Los archivos de registro de CloudTrail pueden contener una o varias entradas de registro. Un evento representa una solicitud específica realizada desde un origen cualquiera, y contiene información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. Los archivos de registro de CloudTrail no rastrean el orden en la pila de las llamadas públicas a la API, por lo que estas no aparecen en ningún orden específico.

En los siguientes ejemplos se muestran entradas de registros de CloudTrail para:

- TerminateCapacityBlocksInstances
- CapacityBlockPaymentFailed
- CapacityBlockScheduled
- CapacityBlockActive
- CapacityBlockFailed
- CapacityBlockExpired

> **Note**
>
> Algunos campos se han eliminado de los ejemplos por motivos de privacidad de datos.

TerminateCapacityBlocksInstances

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "TerminateCapacityBlockInstances",
```

```
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "accountId": "123456789012",
      "type": "AWS::EC2::Instance",
      "ARN": "arn:aws:ec2:US East (N. Virginia):123456789012:instance/
i-1234567890abcdef0"
    }
    {
      "accountId": "123456789012",
      "type": "AWS::EC2::Instance",
      "ARN": "arn:aws::ec2:US East (N. Virginia):123456789012:instance/
i-0598c7d356eba48d7"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      }
}
```


CapacityBlockPaymentFailed


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockPaymentFailed",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
```

```
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:US East (N. Virginia):123456789012:capacity-reservation/
cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "payment-failed"
      }
}
```

CapacityBlockScheduled

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockScheduled",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:US East (N. Virginia):123456789012:capacity-reservation/
cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
```

```
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "scheduled"
      }
}
```

CapacityBlockActive

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockActive",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:US East (N. Virginia):123456789012:capacity-reservation/
cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "active"
      }
 }
```

CapacityBlockFailed


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockFailed",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:US East (N. Virginia):123456789012:capacity-reservation/
cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "failed"
      }
 }
```


CapacityBlockExpired

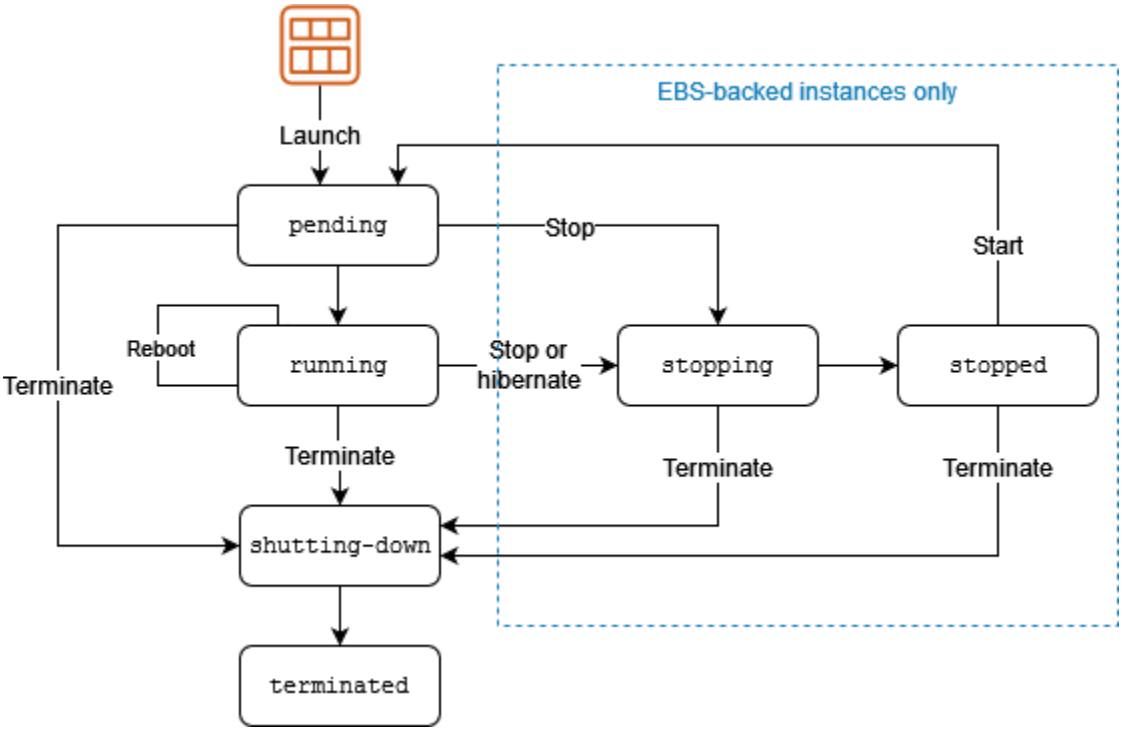

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
```

```
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockExpired",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:US East (N. Virginia):123456789012:capacity-reservation/
cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "expired"
      }
 }
```

Ciclo de vida de la instancia

Una instancia de Amazon EC2 pasa por diferentes estados desde el momento en que la inicia hasta su finalización.

La siguiente ilustración representa las transiciones entre los distintos estados de una instancia. Tenga en cuenta que no se puede detener e iniciar una instancia con respaldo en el almacén de instancias. Para obtener más información acerca de las instancias con respaldo en el almacén de instancias, consulte Almacenamiento para el dispositivo raíz.



En la siguiente tabla, se proporciona una breve descripción de cada estado de la instancia y se indica si se factura. Algunos recursos de AWS, como los volúmenes de Amazon EBS y las direcciones IP elásticas, generan costos con independencia del estado de la instancia. Para obtener más información, consulte Evitar cargos inesperados en la Guía del usuario de AWS Billing.

El estado de la instancia	Descripción	Facturación por uso de instancias
`pending`	La instancia se está preparando para adoptar el estado `running`. Una instancia pasa al estado `pending` cuando se inicia o cuando se reinicia después de tener el estado `stopped`.	No facturado

El estado de la instancia	Descripción	Facturación por uso de instancias
`running`	La instancia está funcionando y ya se puede utilizar.	Facturado
`stopping`	La instancia se está preparando para su detención.	No facturado
`stopped`	La instancia se ha apagado y no se puede usar. La instancia se puede iniciar en cualquier momento.	No facturado
`shutting-down`	La instancia se está preparando para su terminación.	No facturado
`terminated`	La instancia se ha eliminado permanentemente y no se puede iniciar.	No facturado **Note** Las instancias reservadas que se aplicaron a las instancias terminadas se facturan hasta el final del plazo según la opción de pago. Para obtener más información, consulte Reserved Instances

Contenido

- Terminación de la instancia
- Diferencias entre reinicio, detención, hibernación y terminación
- iniciar la instancia
- Detención e iniciación de una instancia de Amazon EC2
- Hibernación de la instancia de Amazon EC2
- Reinicio de su instancia
- Terminación de las instancias de Amazon EC2
- Retirada de instancias
- Resiliencia de las instancias

Lanzamiento de la instancia

Al iniciar una instancia, esta entra en estado `pending`. El tipo de instancia que especificó durante la inicialización determinará el hardware del equipo host para la instancia. Utilizamos la Imagen de máquina de Amazon (AMI) (AMI) que especificó durante la inicialización para reiniciar la instancia. Una vez que la instancia estará lista para utilizarse, entra en estado `running`. Puede conectarse a la instancia en ejecución y usarla como si fuera un equipo.

Tan pronto como la instancia pasa al estado `running`, se factura por cada segundo, con un mínimo de un minuto, que mantenga la instancia en ejecución, aun cuando permanezca inactiva y no se conecte a ella.

Detención e inicio de la instancia (solo instancias respaldadas por Amazon EBS)

Si la instancia no logra hacer una comprobación de estado o no ejecuta las aplicaciones como debería y, si el volumen raíz de la instancia es un volumen de Amazon EBS, puede detener e iniciar la instancia para tratar de solucionar el problema.

Cuando se detiene la instancia, esta entra en estado `stopping` y, a continuación, en estado `stopped`. No se le cobrarán comisiones por uso ni por transferencia de datos por una instancia cuando esté `stopped`. Se cobran cargos por el almacenamiento de cualquier volumen de Amazon EBS. Mientras la estancia está en estado `stopped`, puede modificar ciertos atributos de la misma, incluido el tipo de instancia.

Cuando inicia la instancia, entra en estado `pending` y se transfiere un nuevo equipo host (aunque en algunos casos permanece en el host actual). Cuando se detiene e inicia la instancia, se pierden todos los datos de los volúmenes del almacén de instancias adjuntos al equipo host anterior.

La instancia conserva su dirección IPv4 privada, lo que significa que la dirección IP elástica asociada a la dirección IPv4 privada o la interfaz de red sigue asociada a la instancia. Si la instancia tiene una dirección IPv6, conserva dicha dirección IPv6.

Cada vez que se realiza una transición de una instancia de `stopped` a `running`, se le cobra por segundo mientras la instancia está en ejecución, con un mínimo de un minuto cada vez que se inicia la instancia.

Para obtener más detalles sobre cómo detener e iniciar instancias de base de datos, consulte Detención e iniciación de una instancia de Amazon EC2.

Hibernar instancia (solo instancias con respaldo de Amazon EBS)

Cuando hiberne una instancia, señalaremos el sistema operativo que va a realizar la hibernación (suspensión a disco), que guarda el contenido de la memoria de la instancia (RAM) en su volumen raíz de Amazon EBS. Conservamos el volumen raíz de Amazon EBS de la instancia y cualquier volumen de datos de Amazon EBS asociado. Cuando reinicie su instancia, el volumen raíz de Amazon EBS se restaurará a su estado anterior y el contenido de la RAM se volverá a cargar. Los volúmenes de datos que estaban adjuntos previamente se vuelven a adjuntar y la instancia conserva su ID de instancia.

Cuando hiberne la instancia, esta entrará en estado `stopping` y, a continuación, en estado `stopped`. No se cobra el uso para una instancia hibernada cuando está en el estado `stopped`, pero sí se hace mientras está en el estado `stopping`, a diferencia de lo que ocurre cuando se detiene una instancia sin hibernarla. No cobramos cargos de uso por transferencia de datos, pero sí por el almacenamiento de cualquier volumen de Amazon EBS, incluido el almacenamiento para los datos de la RAM.

Cuando inicia la instancia hibernada, entra en estado `pending` y la movemos a un nuevo equipo host (aunque en algunos casos permanece en el host actual).

La instancia conserva su dirección IPv4 privada, lo que significa que la dirección IP elástica asociada a la dirección IPv4 privada o la interfaz de red sigue asociada a la instancia. Si la instancia tiene una dirección IPv6, conserva dicha dirección IPv6.

Para obtener más información, consulte Hibernación de la instancia de Amazon EC2.

Reinicio de la instancia

Puede reiniciar la instancia con la consola de Amazon EC2, con una herramienta de línea de comandos y con la API de Amazon EC2. Le recomendamos que utilice Amazon EC2 para reiniciar la instancia en lugar de ejecutar el comando de reinicio del sistema operativo desde la instancia.

El reinicio de una instancia es equivalente al reinicio del sistema operativo. La instancia sigue estando en el mismo equipo host y conserva su nombre de DNS público, dirección IP privada y todos los datos en sus volúmenes de almacén de instancias. Normalmente, el reinicio tarda varios minutos en completarse pero el tiempo real dependerá de la configuración de la instancia.

Con el reinicio de una instancia, no se comienza ningún periodo de facturación de la instancia, sino que se continúa la facturación por segundo sin ningún otro cargo mínimo de un minuto.

Para obtener más información, consulte Reinicio de su instancia.

Terminación de la instancia

Si decide que ya no necesita una instancia, puede terminarla. En cuanto el estado de una instancia cambie a `shutting-down` o a `terminated`, dejará de incurrir en costos por ella.

Si habilita la protección de terminación, no puede terminar la instancia con la consola, la CLI ni la API.

Una vez terminada una instancia, permanecerá visible en la consola durante un breve periodo y, a continuación, la entrada se eliminará automáticamente. También puede describir una instancia terminada con la CLI y la API. Los recursos (como las etiquetas) se desvinculan gradualmente de la instancia terminada, por lo que podrían dejar de estar visibles en la instancia terminada tras un breve periodo. No es posible conectarse a una instancia terminada ni recuperarla.

Todas las instancias respaldadas por Amazon EBS admiten el atributo `InstanceInitiatedShutdownBehavior`, que controla si la instancia se detiene o se termina cuando se inicia el apagado desde la propia instancia (por ejemplo, utilizando el comando shutdown en Linux). El comportamiento predeterminado es detener la instancia. Puede modificar la configuración de este atributo mientras la instancia se encuentre en ejecución o detenida.

Cada volumen de Amazon EBS admite el atributo `DeleteOnTermination`, que controla si el volumen se elimina o se mantiene cuando se termina la instancia a la que está adjunto. El comportamiento predeterminado es eliminar el volumen de dispositivo raíz y mantener cualquier otro volumen de EBS.

Para obtener más información, consulte Terminación de las instancias de Amazon EC2.

Diferencias entre reinicio, detención, hibernación y terminación

En la tabla siguiente se resumen las principales diferencias entre el reinicio, la detención, la hibernación y la terminación de la instancia.

Característica	Reinicio	Detención/inicio (solo instancias respaldadas por Amazon EBS)	Hibernar (solo instancias respaldadas por Amazon EBS)	Finalizar
Equipo host	La instancia permanece en el mismo equipo host	Trasladamos la instancia a un nuevo equipo host (aunque en algunos casos, permanece en el host actual).	Trasladamos la instancia a un nuevo equipo host (aunque en algunos casos, permanece en el host actual).	Ninguna
Direcciones IPv4 privadas y públicas	Estas direcciones permanecen igual	La instancia mantiene su dirección IPv4 privada. La instancia obtiene una nueva dirección IPv4 pública, e menos que tenga una dirección IP elástica, la cual no cambia durante la detención ni el inicio.	La instancia mantiene su dirección IPv4 privada. La instancia obtiene una nueva dirección IPv4 pública, e menos que tenga una dirección IP elástica, la cual no cambia durante la detención ni el inicio.	Ninguna
Direcciones IP elásticas (IPv4)	La dirección IP elástica sigue asociada a la instancia	La dirección IP elástica sigue asociada a la instancia	La dirección IP elástica sigue asociada a la instancia	La dirección IP elástica se desvincula de la instancia.

Característica	Reinicio	Detención/inicio (solo instancias respaldadas por Amazon EBS)	Hibernar (solo instancias respaldadas por Amazon EBS)	Finalizar
Dirección IPv6	La instancia mantiene su dirección IPv6	La instancia mantiene su dirección IPv6	La instancia mantiene su dirección IPv6	Ninguna
Volúmenes de almacén de instancias	Los datos se conservan	Los datos se borran	Los datos se borran	Los datos se borran
Volumen de dispositivo raíz	El volumen se conserva	El volumen se conserva	El volumen se conserva	El volumen se elimina de forma predeterminada
RAM (contenido de la memoria)	La RAM se borra.	La RAM se borra.	La RAM se guarda en un archivo en el volumen raíz.	La RAM se borra.

Característica	Reinicio	Detención/inicio (solo instancias respaldadas por Amazon EBS)	Hibernar (solo instancias respaldadas por Amazon EBS)	Finalizar
Facturación	La hora de facturación de instancia no cambia	En cuanto el estado de una instancia cambie a `stopping`, dejará de incurrir en costos por ella. Cada vez que hay una transición de una instancia de `stopped` a `running`, se comienza otro periodo de facturación de la instancia, con un cargo mínimo de un minuto cada vez que se inicia una instancia.	Se cobrarán gastos cuando la instancia esté en el estado `stopping`, pero se dejará de cobrarlos cuando la instancia esté en el estado `stopped`. Cada vez que hay una transición de una instancia de `stopped` a `running`, se comienza otro periodo de facturación de la instancia, con un cargo mínimo de un minuto cada vez que se inicia una instancia.	En cuanto el estado de una instancia cambie a `shutting-down`, dejará de incurrir en costos por ella

Los comandos de apagado del sistema operativo terminan siempre cualquier instancia con respaldo en el almacén de instancias. Puede controlar si los comandos de cierre del sistema operativo detienen o terminan una instancia respaldada por Amazon EBS. Para obtener más información, consulte Cambiar el comportamiento de apagado iniciado por la instancia.

iniciar la instancia

Una instancia es un servidor virtual en la nube de AWS. Una instancia se inicia a partir de una Imagen de máquina de Amazon (AMI) (AMI). La AMI proporciona el sistema operativo, el servidor de aplicaciones y las aplicaciones de la instancia.

Cuando se registra en AWS, puede comenzar a utilizar Amazon EC2 de forma gratuita con el nivel gratuito de AWS. Puede usar la capa gratuita para iniciar y usar una instancia `t2.micro` de forma gratuita durante 12 meses (en regiones donde `t2.micro` no esté disponible, puede usar una instancia `t3.micro` de la capa gratuita). Si inicia una instancia que no está dentro de la capa gratuita, se le cobrará la tarifa de uso estándar de Amazon EC2 por la instancia. Para obtener más información, consulte Precios de Amazon EC2.

Puede iniciar una instancia utilizando los siguientes métodos.

Método	Documentación
[Consola de Amazon EC2] Utilizar el asistente de inicialización de instancias para especificar los parámetros de inicialización.	Lance una instancia con el antiguo asistente de inicialización de instancias
[Consola de Amazon EC2] Crear una plantilla de inicialización e iniciar instancia desde ella.	iniciar una instancia desde una plantilla de inicialización
[Consola de Amazon EC2] Usar una instancia que ya esté disponible como base.	inicialización de una instancia utilizando parámetros de una instancia existente
[Consola de Amazon EC2] Usar una AMI que haya comprado en AWS Marketplace.	iniciar una AWS Marketplace instancia
[AWS CLI] Use una AMI de su elección.	Utilizar Amazon EC2 a través de la AWS CLI
[AWS Tools for Windows PowerShell] Use una AMI de su elección.	Amazon EC2 de AWS Tools for Windows PowerShell
[AWS CLI] Utilice la flota de EC2 para aprovisionar la capacidad en diferentes tipos de instancias de EC2 y zonas de disponibilidad, así como en los modelos de compra de instancia bajo demanda, de instancia reservada e instancia de spot.	Flota de EC2
[AWS CloudFormation] Utilice una plantilla AWS CloudFormation para especificar una instancia.	AWS::EC2::Instance en la Guía del usuario de AWS CloudFormation

Método	Documentación
[AWS SDK] Utilice un AWS SDK específico del idioma para iniciar una instancia.	SDK de AWS para .NET AWS SDK para C++ AWS SDK para Go SDK de AWS para Java SDK de AWS para JavaScript SDK de AWS para PHP V3 SDK de AWS para Python AWS SDK para Ruby V3

Note

Para inicializar una instancia de EC2 en una subred solo de IPv6, debe utilizar instancias integradas en el AWS Nitro System.

Note

Al iniciar una instancia solo de IPv6, es posible que DHCPv6 no proporcione inmediatamente la instancia con el servidor de nombres DNS IPv6. Durante este retraso inicial, es posible que la instancia no sea capaz de resolver dominios públicos.
Para las instancias que se ejecutan en Amazon Linux 2, si desea actualizar inmediatamente el archivo /etc/resolv.conf con el servidor de nombres DNS IPv6, ejecute la siguiente directiva cloud-init durante la inicialización:

```
#cloud-config
bootcmd:
- /usr/bin/sed -i -E 's,^nameserver\s+[\.[:digit:]]+$,nameserver
 fd00:ec2::253,' /etc/resolv.conf
```

Otra opción es cambiar el archivo de configuración y volver a crear la imagen de la AMI de modo que el archivo tenga la dirección del servidor de nombres DNS IPv6 inmediatamente al arrancar.

Al iniciar la instancia, puede iniciarla en una subred asociada a uno de los siguientes recursos:

- Una zona de disponibilidad: esta opción es la predeterminada.
- Una zona local: para iniciar una instancia en una zona local, debe darse de alta en la zona local y, a continuación, crear una subred en la zona. Para obtener más información, consulte Introducción a Zonas locales.
- Una zona de Wavelength: para iniciar una instancia en una zona de Wavelength, debe darse de alta en la zona de Wavelength y, a continuación, crear una subred en la zona. Para obtener información sobre cómo iniciar una instancia en una zona de Wavelength, consulte Introducción a AWS Wavelength.
- Un Outpost: para iniciar una instancia en un Outpost, debe crear un Outpost. Para obtener información acerca de cómo crear un Outpost, consulte Introducción a AWS Outposts.

Después de iniciar la instancia, puede conectarse a ella y utilizarla. Inicialmente, el estado de la instancia es `pending`. Cuando el estado de la instancia es `running`, la instancia ha empezado a arrancar. Puede que transcurran unos instantes antes de que pueda conectarse a la instancia. Tenga en cuenta que los tipos de instancia bare metal pueden tardar más tiempo en iniciarse.

La instancia recibe un nombre de DNS público que puede utilizar para contactar con ella desde Internet. La instancia también recibe un nombre de DNS privado que las demás instancias de la misma VPC pueden utilizar para contactar con ella.

Cuando haya terminado con la instancia, asegúrese de terminarla. Para obtener más información, consulte Terminación de las instancias de Amazon EC2.

Lance una instancia con el nuevo asistente de inicialización de instancias

Puede iniciar una instancia con el nuevo asistente de inicialización de instancias. El asistente de inicialización de instancias especifica todos los parámetros de inicialización necesarios para iniciar una instancia. Si el asistente de inicialización de instancias proporciona un valor predeterminado, puede aceptarlo o especificar su propio valor. Si acepta los valores predeterminados, es posible iniciar una instancia seleccionando solo un par de claves.

> **Important**
>
> Cuando lance una instancia que no pertenece a la capa gratuita de AWS, se le cobrará el tiempo en que la instancia esté funcionando, aunque permanezca inactiva.

Temas

- inicialización rápido de una instancia
- iniciar una instancia mediante parámetros definidos
- Lance una instancia con el antiguo asistente de inicialización de instancias

inicialización rápido de una instancia

Para configurar una instancia rápidamente con fines de prueba, siga estos pasos. Seleccione el sistema operativo y el par de claves y acepte los valores predeterminados. Para obtener información sobre todos los parámetros del asistente de instancia de inicialización, consulte iniciar una instancia mediante parámetros definidos.

Para iniciar rápido una instancia

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la barra de navegación de la parte superior de la pantalla, se muestra la región de AWS actual (por ejemplo, Este de EE. UU. [Ohio]). Seleccione una región en la que se va a iniciar la instancia. Esta elección es importante porque algunos recursos de Amazon EC2 pueden compartirse entre varias regiones, mientras que otros no. Para obtener más información, consulte Ubicaciones de los recursos.
3. En el panel de la consola de Amazon EC2, elija Iniciar instancia.
4. (Opcional) En Name and tags (Nombre y etiquetas), escriba un nombre descriptivo para la instancia en Name (Nombre).
5. En Application and OS Images (Imagen de máquina de Amazon) (Imágenes de aplicaciones y sistema operativo [Imagen de máquina de Amazon]), elija Quick Start (Inicio rápido) y, a continuación, elija el sistema operativo (SO) de la instancia.
6. (Opcional) En Key pair (login) (Par de claves [inicio]), para Key pair name (Nombre de par de claves) seleccione un par de claves existente o cree uno nuevo.
7. En el panel Summary (Resumen), elija Launch instance (Lanzar instancia).

iniciar una instancia mediante parámetros definidos

Excepto por el par de claves, el asistente de inicialización de instancias proporciona valores predeterminados para todos los parámetros. Puede aceptar cualquiera o todos los valores predeterminados, o configurar una instancia al especificar sus propios valores para cada parámetro. Los parámetros se agrupan en el asistente de inicialización de instancias. Las siguientes instrucciones lo guiarán a través de cada grupo de parámetros.

Parámetros de configuración de instancias

- Iniciar la inicialización de una instancia
- Nombre y etiquetas
- Imágenes de aplicaciones y sistema operativo (Imagen de máquina de Amazon)
- Tipo de instancia
- Par de claves (inicio de sesión)
- Network settings (Configuración de red)
- Configurar almacenamiento
- Detalles avanzados
- Resumen

Iniciar la inicialización de una instancia

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la barra de navegación de la parte superior de la pantalla, se muestra la región de AWS actual (por ejemplo, Este de EE. UU. [Ohio]). Seleccione una región en la que se va a iniciar la instancia. Esta elección es importante porque algunos recursos de Amazon EC2 pueden compartirse entre varias regiones, mientras que otros no. Para obtener más información, consulte Ubicaciones de los recursos.
3. En el panel de la consola de Amazon EC2, elija Iniciar instancia.

Nombre y etiquetas

El nombre de la instancia es una etiqueta, donde la clave es Name (Nombre) y el valor es el nombre que especifique. Puede etiquetar la instancia, los volúmenes y las interfaces de red. Para las instancias de spot, solo puede etiquetar la solicitud de instancia de spot. Para obtener más información acerca de las etiquetas, consulte Etiquetar los recursos de Amazon EC2.

Especificar un nombre de instancia y etiquetas adicionales es opcional.

- En Name (Nombre), ingrese un nombre descriptivo para la instancia. Si no especifica un nombre, la instancia se puede identificar mediante su ID, que se genera automáticamente al iniciar la instancia.
- Para agregar otras etiquetas, elija Add additional tag (Agregar etiqueta adicional). Elija Add tag (Agregar etiqueta) y, a continuación, ingrese una clave y un valor, y seleccione el tipo de recurso que desea etiquetar. Elija Add tag (Agregar etiqueta) para cada etiqueta adicional.

Imágenes de aplicaciones y sistema operativo (Imagen de máquina de Amazon)

Una Imagen de máquina de Amazon (AMI) proporciona la información necesaria para crear una instancia. Por ejemplo, una AMI puede contener el software necesario para funcionar como servidor web, como Linux, Apache y su sitio web.

Puede encontrar una AMI adecuada de la siguiente manera: Con cada opción para buscar una AMI, puede elegir Cancel (Cancelar) (en la parte superior derecha) para volver al asistente de instancias de inicialización sin elegir una AMI.

Barra de búsqueda

Para buscar en todas las AMI disponibles, ingrese una palabra clave en la barra de búsqueda de AMI y pulse Enter (Intro). Elija Select (Seleccionar) para seleccionar una AMI.

Recents (Recientes)

Las AMI que se han usado recientemente.

Elija iniciada recientemente o Actualmente en uso y, a continuación, desde Imagen de máquina de Amazon (AMI), seleccione una AMI.

Mis AMI

Las AMI privadas de su propiedad o las AMI privadas que se han compartido con usted.

Elija De mi propiedad o Compartido conmigo y, a continuación, desde Imagen de máquina de Amazon (AMI), seleccione una AMI.

Quick Start (Inicio rápido)

Las AMI están agrupadas por sistema operativo (SO) para ayudar a comenzar rápidamente a trabajar.

En primer lugar, seleccione el sistema operativo que necesita y, a continuación, en Imagen de máquina de Amazon (AMI), seleccione una AMI. Para seleccionar una AMI que sea apta para nivel gratuito, asegúrese de que la AMI esté marcada como Free tier eligible (Apta para nivel gratuito).

Browse more AMIs (Examinar más AMI)

Elija Browse more AMIs (Examinar más AMI) para navegar por el catálogo completo de AMI.

- Para buscar en todas las AMI disponibles, escriba una palabra clave en la barra de búsqueda y pulse Intro.
- Para buscar una AMI mediante un parámetro de Systems Manager, elija el botón de flecha situado a la derecha de la barra de búsqueda y, a continuación, Search by Systems Manager parameter (Buscar por parámetro de Systems Manager). Para obtener más información, consulte Cómo buscar una AMI con un parámetro de Systems Manager.
- Para buscar por categoría, elija Quickstart AMIs (AMI de inicio rápido), My AMIs (Mis AMI), AWS Marketplace AMIs (AMI) o Community AMIs (AMI de comunidad).

  AWS Marketplace es una tienda en línea donde puede comprar el software que se ejecuta en AWS, incluidas las AMI. Para obtener más información sobre cómo iniciar una instancia desde AWS Marketplace, consulte iniciar una AWS Marketplace instancia. En Community AMIs (AMI de comunidad), puede encontrar las AMI que los miembros de la comunidad de AWS han puesto a disposición de los demás. Las AMI de Amazon o de un socio verificado están marcadas como Verified provider (Proveedor verificado).
- Para filtrar la lista de AMI, active una o varias casillas de verificación en Refine results (Refinar los resultados) a la izquierda de la pantalla. Las opciones de filtro son diferentes en función de la categoría de búsqueda seleccionada.
- Compruebe la lista Tipo de dispositivo raíz que se muestra para cada AMI. Observe cuáles son las AMI del tipo que necesita, ebs (respaldadas por Amazon EBS) o bien instance-store (con respaldo en el almacén de instancias). Para obtener más información, consulte Almacenamiento para el dispositivo raíz.
- Compruebe la lista Tipo de virtualización que se muestra para cada AMI. Observe cuáles son las AMI del tipo que necesita, hvm o paravirtual. Por ejemplo, algunos tipos de instancias requieren una HVM. Para obtener más información sobre los tipos de virtualización de Linux, consulte Tipos de virtualización de AMI.
- Compruebe el modo de arranque que aparece para cada AMI. Observe qué AMI utiliza el modo de arranque que necesita: legacy-bios, uefi o uefi-preferred. Para obtener más información, consulte Modos de arranque de Amazon EC2.

- Elija una AMI que satisfaga sus necesidades y, a continuación, elija Seleccionar.

Advertencia al cambiar la AMI

Si modifica la configuración de los volúmenes o grupos de seguridad asociados a la AMI seleccionada y, a continuación, elige una AMI diferente, se abre una ventana para avisarle que se modificarán o eliminarán algunas de las configuraciones actuales. Puede revisar los cambios en los volúmenes y grupos de seguridad. Además, puede ver qué volúmenes se agregarán y eliminarán, o ver únicamente los volúmenes que se agregarán.

Tipo de instancia

El tipo de instancia define la configuración de hardware y el tamaño de la instancia. Los tipos de instancia más grandes tienen una CPU y memoria superiores. Para obtener más información, consulte Tipos de instancias de Amazon EC2.

- En Instance Type (Tipo de instancia), seleccione el tipo de instancia de la instancia.

  Nivel gratuito: si la cuenta de AWS tiene menos de 12 meses de antigüedad, puede utilizar Amazon EC2 en el nivel gratuito si selecciona el tipo de instancia t2.micro (o el tipo de instancia t3.micro en las regiones donde t2.micro no esté disponible). Si un tipo de instancia es elegible para el nivel gratuito, tiene la etiqueta Elegible para el nivel gratuito. Para obtener más información acerca de t2.micro y t3.micro, consulte Instancias de rendimiento ampliable.
- Comparación de tipos de instancia: puede comparar distintos tipos de instancia mediante los siguientes atributos: número de vCPU, arquitectura, cantidad de memoria (GiB), cantidad de almacenamiento (GB), tipo de almacenamiento y rendimiento de red.
- Obtener asesoramiento: puede obtener orientación y sugerencias sobre tipos de instancias en el selector de tipos de instancias de EC2 de Amazon Q. Para obtener más información, consulte Obtención de recomendaciones de tipos de instancias para una nueva carga de trabajo.

Par de claves (inicio de sesión)

En Key pair name (Nombre de par de claves) seleccione un par de claves existente o seleccione Create new key pair (Crear nuevo par de claves) para crear uno nuevo. Para obtener más información, consulte Pares de claves e instancias de Amazon EC2.

> **Important**
>
> Si elige la opción Proceed without key pair (Not recommended) (Continuar sin un par de claves [No recomendado]), no podrá conectarse a la instancia a menos que elija una AMI que esté configurada para ofrecer a los usuarios otra forma de iniciar sesión.

Network settings (Configuración de red)

Establezca la configuración de red, según sea necesario.

- VPC: elige una VPC existente para la instancia. Puede elegir la VPC predeterminada o una que haya creado. Para obtener más información, consulte the section called “Nubes virtuales privadas”.
- Subnet (Subred): puede iniciar una instancia en una subred asociada con una zona de disponibilidad, zona local, zona Wavelength u Outpost.

  Para iniciar la instancia en una zona de disponibilidad, seleccione la subred en la que desea iniciar la instancia. Para crear una subred, elija Crear nueva subred para ir a la consola de Amazon VPC. Cuando haya terminado, vuelva al asistente de inicialización de instancias y elija el ícono Refresh (Actualizar) para cargar la subred en la lista.

  Todas las instancias que lance en una subred solo de IPv6 deben ser instancias integradas en el sistema Nitro.

  Para iniciar la instancia en una zona local, seleccione una subred que haya creado en la zona local.

  Para iniciar una instancia en un Outpost, seleccione una subred en una VPC que haya asociado a un Outpost.
- Asignar IP pública automáticamente: especifique si la instancia recibe una dirección IPv4 pública. De forma predeterminada, las instancias en una subred predeterminada reciben una dirección IPv4 pública, mientras que las instancias en una subred no predeterminada no la reciben. Puede seleccionar Habilitar o Deshabilitar para anular la configuración predeterminada de la subred. Para obtener más información, consulte Direcciones IPv4 públicas.
- Firewall (Grupos de seguridad): utilice un grupo de seguridad para definir reglas de firewall para la instancia. Estas reglas especifican qué tráfico procedente de la red se entregará en la instancia. El resto del tráfico se ignora. Para obtener más información acerca de los grupos de seguridad, consulte Grupos de seguridad de Amazon EC2 para instancias EC2.

Si agrega una interfaz de red, debe incluir el mismo grupo de seguridad en la interaz de red.

Seleccione o cree un grupo de seguridad como se indica a continuación:

- Para seleccionar un grupo de seguridad existente para su VPC, elija Select existing security group (Seleccionar un grupo de seguridad existente) y seleccione el grupo de seguridad en Common security groups (Grupos de seguridad comunes).
- Elija Create security group (Crear grupo de seguridad) para crear un nuevo grupo de seguridad de VPC. El asistente de inicialización de instancias define automáticamente el grupo de seguridad de launch-wizard-x y proporciona las siguientes casillas de verificación para agregar rápidamente reglas del grupo de seguridad:

  (Linux) Permitir tráfico SSH desde: crea una regla de entrada que le permite conectarse a la instancia mediante SSH (puerto 22).

  (Windows) Permitir tráfico SSH desde: crea una regla de entrada que le permite conectarse a la instancia mediante RDP (puerto 3389).

  Especifique si el tráfico proviene de Anywhere (Cualquier lugar), Custom (Personalizado) o My IP (Mi dirección IP).

  Allow HTTPs traffic from the internet (Permitir tráfico HTTPS desde Internet): crea una regla de entrada que abre el puerto 443 (HTTPS) para permitir el tráfico de Internet desde cualquier lugar. Necesitará esta regla si la instancia va a ser un servidor web.

  Allow HTTP traffic from the internet (Permitir el tráfico HTTP desde Internet): crea una regla de entrada que abre el puerto 80 (HTTP) para permitir el tráfico de Internet desde cualquier lugar. Necesitará esta regla si la instancia va a ser un servidor web.

  Puede editar estas reglas para adaptarse a sus necesidades.

  Para editar o agregar una regla, elija Edit (Editar), en la parte superior derecha. Para agregar una regla, elija Add security group rule (Agregar regla de grupo de seguridad). En Type (Tipo), seleccione el tipo de tráfico de red. El campo Protocol (Protocolo) se rellena automáticamente con el protocolo para abrir al tráfico de red. En Source type (Tipo de origen) elija un tipo de origen. Para permitir que el asistente de inicialización de instancias agregue la dirección IP pública de su computadora, elija My IP (Mi IP). Sin embargo, si se conecta a través de un ISP o protegido por su firewall sin una dirección IP estática, deberá encontrar el rango de direcciones IP utilizadas por los equipos cliente.

> **Warning**
>
> Las reglas que habilitan a todas las direcciones IP (`0.0.0.0/0`) para que puedan acceder a su instancia por SSH o RDP son aceptables si está por iniciar una instancia de prueba por un breve periodo y la detendrá o finalizará pronto, pero no es seguro para entornos de producción. Debe autorizar el acceso a su instancia únicamente a una dirección IP o a un rango de direcciones IP específico.

- Configuración avanzada de red: disponible solo si elige una subred.

  Interfaz de red

  - Índice de dispositivo: es el índice de la tarjeta de red. La interfaz de red principal debe asignarse al índice 0 de la tarjeta de red. Algunos tipos de instancia admiten varias tarjetas de red.
  - Interfaz de red: seleccione Nueva interfaz para permitir que Amazon EC2 cree una interfaz nueva o seleccione una interfaz de red existente disponible.
  - Descripción: (Opcional) una descripción para la nueva interfaz de red.
  - Subnet (Subred): la subred en la que se creará una nueva interfaz de red. Para la interfaz de red principal (`eth0`), esta es la subred en la que se inicia la instancia. Si ha especificado una interfaz de red para `eth0`, se inicia la instancia en la subred en la que se encuentra la interfaz de red.
  - Grupos de seguridad: uno o más grupos de seguridad de la VPC a los que asociar la interfaz de red.
  - IP principal: una dirección IPv4 privada del intervalo de su subred. Deje en blanco para permitir que Amazon EC2 elija una dirección IPv4 privada.
  - Secondary IP (IP secundaria): una o más direcciones IPv4 privadas del intervalo de la subred. Elija Manually assign (Asignar manualmente) e ingrese una dirección IP. Elija Add IP (Agregar IP) para agregar otra dirección IP. O bien, elija Asignar automáticamente para permitir que Amazon EC2 elija uno por usted e ingrese un valor para indicar el número de direcciones IP que desea agregar.
  - (Solo IPv6) IPv6 IPs (IP IPv6): una dirección IPv6 del intervalo de la subred. Elija Manually assign (Asignar manualmente) e ingrese una dirección IP. Elija Add IP (Agregar IP) para agregar otra dirección IP. O bien, elija Asignar automáticamente para permitir que Amazon EC2 elija uno por usted e ingrese un valor para indicar el número de direcciones IP que desea agregar.
  - Prefijos IPv4: los prefijos IPv4 para la interfaz de red.
  - Prefijos IPv6: los prefijos IPv6 para la interfaz de red.

- (Doble pila y solo IPv6) Asignar la IP IPv6 principal: (opcional) si va a iniciar una instancia en una subred de doble pila o solo para IPv6, tiene la opción de asignar la IP IPv6 principal. La asignación de una dirección IPv6 principal le permite evitar interrumpir el tráfico a las instancias o ENI. Elija Habilitar si esta instancia depende de que su dirección IPv6 no cambie. Al iniciar la instancia, AWS asignará automáticamente una dirección IPv6 asociada al ENI adjunto a la instancia como la dirección IPv6 principal. Una vez que habilite una dirección GUA de IPv6 para que sea la IPv6 principal, no podrá deshabilitarla. Al habilitar una dirección GUA de IPv6 para que sea una de IPv6 principal, la primera dirección GUA de IPv6 pasará a ser la dirección IPv6 principal hasta que se termine la instancia o se separe la interfaz de red. Si tiene varias direcciones IPv6 asociadas a un ENI adjunto a su instancia y habilita una dirección IPv6 principal, la primera dirección GUA de IPv6 asociada al ENI pasa a ser la dirección IPv6 principal.
- Eliminar al terminar: si la interfaz de red se elimina, cuándo se elimina la instancia.
- Elastic Fabric Adapter: indica si la interfaz de red es un Elastic Fabric Adapter. Para obtener más información, consulte Elastic Fabric Adapter.
- ENA Express: ENA Express funciona con la tecnología de Scalable Reliable Datagram (SRD) de AWS. La tecnología SRD utiliza un mecanismo de difusión de paquetes para distribuir la carga y evitar la congestión de la red. Al habilitar ENA Express, las instancias compatibles se comunican mediante SRD además del tráfico de TCP normal siempre que sea posible. El asistente de inicialización de instancias no incluye la configuración de ENA Express para la instancia, a menos que seleccione Habilitar o Deshabilitar en la lista.
- UDP de ENA Express: si habilitó ENA Express, de forma opcional, puede usar dicha característica para el tráfico de UDP. El asistente de inicialización de instancias no incluye la configuración de ENA Express para la instancia, a menos que seleccione Habilitar o Deshabilitar.

Elija Agregar interfaz de red para agregar interfaces de la red adicionales. Las interfaces de red adicionales pueden residir en una subred distinta de la misma VPC o en una subred de una VPC diferente que posea (siempre que la subred se encuentre en la misma zona de disponibilidad que la instancia). Si decide añadir una interfaz de red adicional que resida en otra subred de VPC, verá la opción Subredes de varias VPC al seleccionar una subred. Si selecciona una subred en otra VPC, la etiqueta de varias VPC se muestra junto a la interfaz de red que ha añadido. Esto le permite crear instancias con varios hosts en las VPC con diferentes configuraciones de red y seguridad. Tenga en cuenta que si adjunta una ENI adicional desde otra VPC, debe elegir un grupo de seguridad para la ENI desde esa VPC.

Para obtener más información, consulte Interfaces de red elásticas. Si especifica más de una interfaz de red, la instancia no puede recibir una dirección IPv4 pública. Además, si especifica una interfaz de red existente para eth0, no puede anular la configuración de la IPv4 pública de la subred con Auto-assign Public IP (Asignar IP pública automáticamente). Para obtener más información, consulte Asignar una dirección IPv4 pública durante la inicialización de la instancia.

Configurar almacenamiento

La AMI seleccionada incluye uno o más volúmenes de almacenamiento, incluido el volumen de dispositivo raíz. Se pueden especificar volúmenes adicionales para adjuntar a la instancia.

Se puede utilizar la vista Simple o Advanced (Avanzada). Con la vista Simple, especifica el tamaño y el tipo de volumen. Para especificar todos los parámetros de volumen, elija la vista Advanced (Avanzada) (en la parte superior derecha de la tarjeta).

Mediante el uso de la vista Advanced (Avanzada), puede configurar cada volumen de la siguiente manera:

- Storage type (Tipo de volumen): seleccione el almacén de instancias o los volúmenes de Amazon EBS que desea asociar a la instancia. Los tipos de volumen disponibles en la lista dependen del tipo de instancia que haya elegido. Para obtener más información, consulte Almacén de instancias Amazon EC2 y Volúmenes de Amazon EBS.
- Device name (Nombre de dispositivo): selecciónelo de la lista de nombres de dispositivo disponibles para el volumen.
- Snapshot (Instantánea): seleccione la instantánea desde la que desea restaurar un volumen. También puede buscar instantáneas públicas y compartidas disponibles escribiendo texto en el campo Snapshot (Instantánea).
- Size (GiB) (Tamaño [GiB]): para volúmenes de EBS, puede especificar un tamaño de almacenamiento. Si ha seleccionado una AMI y una instancia aptas para el nivel gratuito, recuerde que para permanecer en dicho nivel debe mantenerse por debajo de los 30 GiB de almacenamiento total.
- Volume type (Tipo de volumen): elija un tipo de volumen para volúmenes de EBS. Para obtener más información, consulte Tipos de volúmenes de Amazon EBS en la Guía del usuario de Amazon EBS.
- IOPS: si ha seleccionado un tipo de volumen Provisioned IOPS SSD, puede ingresar el número de operaciones de E/S por segundo (IOPS) que puede soportar el volumen.

- Delete on termination (Eliminar al terminar): para los volúmenes de Amazon EBS, elija Yes (Sí) si se eliminará el volumen cuando se termine la instancia asociada o elija No para mantener el volumen. Para obtener más información, consulte Conservación de los datos cuando se termina una instancia.
- Encrypted (Cifrado): si el tipo de instancia admite el cifrado EBS, puede elegir Yes (Sí) para habilitar el cifrado para el volumen. Si ha habilitado el cifrado de forma predeterminada en esta región, el cifrado se habilita automáticamente. Para obtener más información, consulte Cifrado de Amazon EBS en la Guía del usuario de Amazon EBS.
- KMS key (Clave KMS): si ha seleccionado Yes (Sí) para Encrypted (Cifrado), a continuación, debe seleccionar una clave administrada por el cliente a fin de utilizarla para cifrar el volumen. Si ha habilitado el cifrado de forma predeterminada en esta región, se selecciona automáticamente la clave predeterminada administrada por el cliente. Puede seleccionar una clave diferente o especificar el ARN de cualquier clave administrada por el cliente que haya creado.
- Sistemas de archivos: monte un sistema de archivos de Amazon EFS o Amazon FSx en la instancia. Para obtener más información sobre cómo montar un sistema de archivos de Amazon EFS, consulte Uso de Amazon EFS con instancias de Linux. Para obtener más información sobre cómo montar un sistema de archivos de Amazon FSx, consulte Uso de Amazon FSx con Amazon EC2.

Detalles avanzados

En Detalles avanzados, expanda la sección para ver los campos y especifique cualquier parámetro adicional para la instancia.

- Purchasing option (Opción de compra): elija Request Spot Instances (Solicitar instancias de spot) para solicitar instancias de spot al precio de spot, limitado al precio bajo demanda, y elija Customize (Personalizar) para cambiar la configuración de instancia de spot predeterminada. Puede establecer el precio máximo (no recomendado) y cambiar el tipo de solicitud, la duración de la solicitud y el comportamiento de interrupción. Si no solicita una instancia de spot, Amazon EC2 inicia una instancia bajo demanda de forma predeterminada. Para obtener más información, consulte Crear una solicitud de instancia de spot.
- Directorio de unión al dominio: seleccione el directorio de AWS Directory Service (dominio) al que se ha unido la instancia después del lanzamiento. Si selecciona un dominio, debe seleccionar un rol de IAM con los permisos necesarios. Para obtener más información sobre dominios que unen instancias de Linux, consulte Unir fácilmente una instancia de Linux EC2 a su directorio de Microsoft AD administrado de AWS. Para obtener más información sobre dominios que unen

instancias de Windows, consulte Unir fácilmente una instancia de Windows EC2 a su directorio de Microsoft AD administrado de AWS.

- IAM instance profile (Perfil de instancias de IAM): seleccione un perfil de instancias de AWS Identity and Access Management (IAM) para asociarlo a la instancia. Para obtener más información, consulte Roles de IAM para Amazon EC2.
- Hostname type (Tipo de nombre de anfitrión): selecciónelo si desea que el nombre de host del sistema operativo invitado de la instancia incluya el nombre del recurso o el nombre de IP. Para obtener más información, consulte Tipos de nombres de host de instancias de Amazon EC2.
- DNS Hostname (Nombre de host DNS): determina si las consultas de DNS al nombre del recurso o de IP (según lo que haya seleccionado para Hostname type) responderán con la dirección IPv4 (registro A), dirección IPv6 (registro AAAA) o ambas. Para obtener más información, consulte Tipos de nombres de host de instancias de Amazon EC2.
- Shutdown behavior (Comportamiento de cierre): seleccione si la instancia debe detenerse o terminarse al cerrarla. Para obtener más información, consulte Cambiar el comportamiento de apagado iniciado por la instancia.
- Stop - Hibernate behavior (Detener: comportamiento de hibernación): para habilitar la hibernación, seleccione Enable (Habilitar). Este campo solo está disponible si la instancia satisface los requisitos previos de hibernación. Para obtener más información, consulte Hibernación de la instancia de Amazon EC2.
- Termination protection (Protección de terminación): para evitar una terminación accidental, elija Enable (Habilitar). Para obtener más información, consulte Cómo habilitar la protección contra la terminación.
- Protección de detención: para evitar detenciones accidentales, elija Enable (Habilitar). Para obtener más información, consulte Habilitación de la protección de detención.
- Detailed CloudWatch monitoring (Supervisión detallada de CloudWatch): elija Enable (Habilitar) para activar la supervisión detallada de la instancia con Amazon CloudWatch. Se aplican cargos adicionales. Para obtener más información, consulte Monitorear las instancias con CloudWatch.
- GPU elástica: Amazon Elastic Graphics llegó al final de su vida útil el 8 de enero de 2024. Para las cargas de trabajo que requieren aceleración de gráficos, le recomendamos usar instancias G4ad, G4dn o G5 de Amazon EC2.
- Inferencia elástica: acelerador de Elastic Inference a asociar a su instancia CPU EC2. Para obtener más información, consulte la sección sobre cómo trabajar con Amazon Elastic Inference en la guía para desarrolladores de Amazon Elastic Inference.

> **Note**
>
> A partir del 15 de abril de 2023, AWS no incorporará nuevos clientes a Amazon Elastic Inference (EI) y ayudará a los clientes actuales a migrar sus cargas de trabajo a opciones que ofrezcan un mejor precio y rendimiento. A partir del 15 de abril de 2023, los nuevos clientes no podrán iniciar instancias con los aceleradores de Amazon EI en Amazon SageMaker, Amazon ECS o Amazon EC2. Sin embargo, los clientes que hayan utilizado Amazon EI al menos una vez durante los últimos 30 días se consideran clientes actuales y podrán seguir utilizando el servicio.

- Credit specification (Especificación de crédito): elija Unlimited (Ilimitado) para permitir que las aplicaciones se expandan más allá de la base de referencia por el tiempo que sea necesario. Este campo solo es válido para instancias T. Podrían aplicarse cargos adicionales. Para obtener más información, consulte Instancias de rendimiento ampliable.
- Nombre del grupo de ubicación: especifique el grupo de ubicación en el que desea iniciar la instancia. Se puede seleccionar un grupo de ubicación existente o crear uno nuevo. No todos los tipos de instancia admiten la inicialización de instancias en un grupo de ubicación. Para obtener más información, consulte Grupos de ubicación.
- EBS-optimized instance (instancia optimizada para EBS): una instancia optimizada para Amazon EBS utiliza una pila de configuración optimizada y proporciona capacidad dedicada adicional para la E/S de Amazon EBS. Si el tipo de instancia admite esta característica, seleccione Enable (Habilitar) para habilitarla. Se aplican cargos adicionales. Para obtener más información, consulte the section called “Optimización de EBS”.
- Capacity Reservation (Reserva de capacidad): especifique si desea iniciar la instancia en cualquier reserva de capacidad abierta (Open [Abierta]), una reserva de capacidad específica (Target by ID [Destino por ID]) o un grupo de reserva de capacidad (Target by group [Destino por grupo]). Para especificar que no se debe utilizar una reserva de capacidad, elija None (Ninguna). Para obtener más información, consulte iniciar instancias en una Reserva de capacidad existente.
- Tenancy (Tenencia): elija si ejecutar su instancia en hardware compartido (Shared [Compartido]), asilado, hardware dedicado (Dedicated [Dedicado]) o en un host dedicado (Dedicated host [Host dedicado]). Si decide iniciar la instancia en host dedicado, puede especificar si desea iniciar la instancia en un grupo de recursos de host o utilizar un host dedicado específico como destino. Podrían aplicarse cargos adicionales. Para obtener más información, consulte Dedicated Instances y Dedicated Hosts.

- RAM disk ID (ID de disco RAM): (solo válido para AMI paravirtuales [PV]) seleccione un disco RAM para la instancia. Si ha seleccionado un kernel, puede que tenga que seleccionar un disco RAM específico con los controladores necesarios.
- Kernel ID (ID del kernel): (solo válido para AMI paravirtuales [PV]) seleccione un kernel para la instancia.
- Nitro Enclave: permite crear entornos de ejecución aislados, llamados enclaves, a partir de instancias de Amazon EC2. Seleccione Enable (Habilitar) para habilitar la instancia de Nitro Enclaves de AWS. Para obtener más información, consulte ¿Qué son los Nitro Enclaves de AWS? en la Guía del usuario de Nitro Enclaves de AWS.
- Configuraciones de licencia: puede iniciar instancias con la configuración de licencia especificada para realizar un seguimiento del uso de la licencia. Para obtener más información, consulte la sección Crear configuraciones de licencia en la Guía del usuario de License Manager de AWS.
- Metadata accessible (Metadatos accesibles): puede habilitar o deshabilitar el acceso a los metadatos de instancia. Para obtener más información, consulte Configurar las opciones de metadatos para instancias nuevas.
- Punto de conexión IPv6 para la obtención de metadatos: puede permitir que una instancia utilice la dirección IPv6 del IMDS `[fd00:ec2::254]` para recuperar los metadatos de la instancia. Esta opción solo está disponible para el lanzamiento de instancias basadas en AWS Nitro System en una subred compatible con IPv6 (de doble pila o solo IPv6). Para obtener más información sobre cómo recuperar los metadatos de las instancias, consulte Recuperar metadatos de instancia.
- Metadata version (Versión de metadatos): si habilita el acceso a los metadatos de instancia, puede optar por requerir el uso de Servicio de metadatos de instancia, versión 2, al solicitar metadatos de instancia. Para obtener más información, consulte Configurar las opciones de metadatos para instancias nuevas.
- Límite de saltos de respuesta de metadatos: si habilita metadatos de instancia, puede establecer el número permitido de saltos de red para el token de metadatos. Para obtener más información, consulte Configurar las opciones de metadatos para instancias nuevas.
- Allow tags in metadata (Permitir etiquetas en metadatos): si selecciona Enable (Habilitar), la instancia permitirá acceder a todas sus etiquetas desde sus metadatos. Si no se especifica ningún valor, entonces, de forma predeterminada, no se permitirá el acceso a las etiquetas en los metadatos de instancia. Para obtener más información, consulte Permitir acceso a etiquetas en metadatos de instancia.
- User data (Datos de usuario): puede especificar los datos de usuario para configurar una instancia durante la inicialización o para ejecutar un script de configuración. Para obtener más información sobre los datos del usuario para las instancias de Linux, consulte Ejecución de comandos en la

instancia de Amazon EC2 durante la inicialización. Para obtener más información sobre los datos del usuario para las instancias de Windows, consulte Cómo gestiona Amazon EC2 los datos de usuario de las instancias de Windows.

Resumen

Utilice el panel Summary (Resumen) para especificar el número de instancias que se van a iniciar, revisar la configuración de las instancias y iniciar las instancias.

- Number of instances (Número de instancias): escriba el número de instancias que desea iniciar. Todas las instancias se iniciarán con la misma configuración.

  > **Tip**
  >
  > Para garantizar inicializacións de instancias más rápidos, divida las solicitudes de gran tamaño en lotes más pequeños. Por ejemplo, cree cinco solicitudes de inicialización independientes para 100 instancias cada una en lugar de una solicitud de inicialización para 500 instancias.

- (Opcional) Si especifica más de una instancia, para asegurarse de que se mantenga el número correcto de instancias para satisfacer la demanda de la aplicación, puede elegir Considerar escalado automático de EC2 para crear una plantilla de inicialización y un grupo de escalado automático. Auto Scaling escala el número de instancias en el grupo según sus especificaciones. Para obtener más información, consulte la Guía del usuario de Amazon EC2 Auto Scaling.

  > **Note**
  >
  > Si Amazon EC2 Auto Scaling marca una instancia que está en un grupo de escalado automático como incorrecta, la instancia se programará automáticamente para su reemplazo cuando se termine y se lance otra, y se pierden los datos de la instancia original. Una instancia se marca como incorrecta si detiene o reinicia la instancia o si otro evento marca la instancia como incorrecta. Para obtener más información, consulte Comprobaciones de estado para instancias en un grupo de escalado automático en la Guía del usuario de Amazon EC2 Auto Scaling.

- Revise los detalles de la instancia y haga los cambios necesarios. Puede navegar directamente a una sección si selecciona el enlace correspondiente en el panel Summary (Resumen).
- Cuando esté listo para iniciar una instancia, elija Launch instance (iniciar instancia).

Si se produce un error al iniciar la instancia o el estado pasa inmediatamente a `terminated` en lugar de `running`, consulte Solucionar problemas de lanzamiento de instancias.

(Opcional) Puede crear una alerta de facturación para la instancia. En la pantalla de confirmación, en Next Steps (Próximos pasos), elija Create billing alerts (Crear alertas de facturación) y siga las instrucciones. También se pueden crear alertas de facturación después de iniciar la instancia. Para obtener más información, consulte Creación de una alarma de facturación para supervisar los cargos estimados de AWS en la Guía del usuario de Amazon CloudWatch.

Lance una instancia con el antiguo asistente de inicialización de instancias

Puede iniciar una instancia con el antiguo asistente de inicialización de instancias solo si su región admite la experiencia de inicialización anterior. El launch wizard de instancias especifica todos los parámetros de inicialización necesarios para iniciar una instancia. Si el launch wizard de instancias proporciona un valor predeterminado, puede aceptarlo o especificar su propio valor. Debe especificar una AMI y un par de claves al iniciar una instancia.

Para obtener las instrucciones de uso del nuevoasistente de inicialización de instancias, consulte Lance una instancia con el nuevo asistente de inicialización de instancias.

> **Important**
>
> Cuando lance una instancia que no pertenece a la capa gratuita de AWS, se le cobrará el tiempo en que la instancia esté funcionando, aunque permanezca inactiva.

Pasos para iniciar una instancia

- Iniciar la inicialización de una instancia
- Paso 1: Elegir una Imagen de máquina de Amazon (AMI)
- Paso 2: Elegir un tipo de instancia
- Paso 3: Configurar los detalles de la instancia
- Paso 4: Agregar almacenamiento
- Paso 5: Añadir etiquetas
- Paso 6: Configurar un grupo de seguridad
- Paso 7: Revisar la inicialización de la instancia y seleccionar el par de claves

Iniciar la inicialización de una instancia

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la barra de navegación de la parte superior de la pantalla, se muestra la región actual (por ejemplo, US East (Ohio)). Seleccione una región para la instancia adecuada a sus necesidades. Esta elección es importante porque algunos recursos de Amazon EC2 pueden compartirse entre varias regiones, mientras que otros no. Para obtener más información, consulte Ubicaciones de los recursos.
3. En el panel de la consola de Amazon EC2, elija Iniciar instancia.

Paso 1: Elegir una Imagen de máquina de Amazon (AMI)

Cuando inicia una instancia, debe seleccionar una configuración, denominada Imagen de máquina de Amazon (AMI). Una AMI contiene la información necesaria para crear una nueva instancia. Por ejemplo, una AMI puede contener el software necesario para funcionar como servidor web, como Linux, Apache y su sitio web.

Al iniciar una instancia, puede seleccionar una AMI de la lista o seleccionar un parámetro Systems Manager que apunte a un ID de AMI. Para obtener más información, consulte the section called "Cómo buscar una AMI con un parámetro de Systems Manager".

En la página Elegir una imagen de máquina de Amazon (AMI), utilice una de las dos opciones para elegir una AMI. Busque en la lista de AMI o busque por parámetro Administrador de sistemas.

Buscando en la lista de AMI

1. Seleccione el tipo de AMI a utilizar en el panel izquierdo:

   Quick Start (Inicio rápido)

   Una selección de AMI populares que le ayudan a empezar a trabajar rápidamente. Para seleccionar una AMI que sea apta para la capa gratuita, elija Free tier only (Solo capa gratuita) en panel izquierdo. Estas AMI están marcadas como Free tier eligible (Apta para la capa gratuita).

   Mis AMI

   Las AMI privadas de su propiedad o las AMI privadas que se han compartido con usted. Para ver las AMI compartidas con usted, elija Shared with me (Compartidas conmigo) en el panel izquierdo.

AWS Marketplace

Una tienda online donde puede comprar el software que se ejecuta en AWS, incluidas las AMI. Para obtener más información sobre cómo iniciar una instancia desde AWS Marketplace, consulte iniciar una AWS Marketplace instancia.

Community AMIs (AMI de comunidad)

Las AMI que los miembros de la comunidad de AWS han puesto a disposición de los demás. Para filtrar la lista de las AMI por sistema operativo, elija la casilla apropiada en Operating system (Sistema operativo). También puede filtrar por tipo de arquitectura y de dispositivo raíz.

2. (Instancias de Linux) Compruebe la lista Tipo de dispositivo raíz que se muestra para cada AMI. Observe qué AMI son del tipo que necesita, `ebs` (respaldadas por Amazon EBS) o bien `instance-store` (con respaldo en el almacén de instancias). Para obtener más información, consulte Almacenamiento para el dispositivo raíz.
3. Compruebe la lista Virtualization type (Tipo de virtualización) que se muestra para cada AMI. Observe qué AMI son del tipo que necesita, `hvm` o bien `paravirtual`. Por ejemplo, algunos tipos de instancias requieren una HVM. Para obtener más información sobre los tipos de virtualización de Linux, consulte Tipos de virtualización de AMI.
4. Compruebe el modo de arranque que aparece para cada AMI. Observe cuál AMI utiliza el modo de arranque que necesita, `legacy-bios` o `uefi`. Para obtener más información, consulte Modos de arranque de Amazon EC2.
5. Elija una AMI que satisfaga sus necesidades y, a continuación, elija Select (Seleccionar).

Por parámetro Systems Manager

1. Elija Search by Administrador de sistemas parameter (Buscar por parámetro de Administrador de sistemas) (en la parte superior derecha).
2. Para Systems Manager parameter (Parámetro de Systems Manager), seleccione un parámetro. El ID de AMI correspondiente aparece junto a Actualmente se resuelve en.
3. Elija Search (Buscar). Las AMI que coinciden con el ID de AMI aparecen en la lista.
4. Seleccione la AMI de la lista y elija Select (Seleccionar).

Paso 2: Elegir un tipo de instancia

En la página Choose an Instance Type (Elegir un tipo de instancia), seleccione la configuración de hardware y el tamaño de la instancia que se va a iniciar. Los tipo de instancia más grandes tienen una CPU y memoria superiores. Para obtener más información, consulte Tipos de instancias de Amazon EC2.

Para seguir siendo elegible para la capa gratuita, elija el tipo de instancia t2.micro (o el tipo de instancia t3.micro en Regiones, donde t2.micro no está disponible). Si un tipo de instancia es elegible para el nivel gratuito, tiene la etiqueta Elegible para el nivel gratuito. Para obtener más información acerca de t2.micro y t3.micro, consulte Instancias de rendimiento ampliable.

De forma predeterminada, el asistente muestra los tipos de instancias de la generación actual y selecciona el primer tipo de instancia disponible en función de la AMI que ha seleccionado. Para ver los tipos de instancias de generaciones anteriores, elija All generations (Todas las generaciones) en la lista de filtros.

> **Note**
>
> Para configurar rápidamente una instancia para realizar pruebas, elija Review and Launch (Revisar y iniciar) para aceptar la configuración predeterminada y iniciar la instancia. De lo contrario, para configurar otros ajustes de la instancia, elija Next: Configure Instance Details (Siguiente: Configurar detalles de instancia).

Paso 3: Configurar los detalles de la instancia

En la página Configure Instance Details (Configurar detalles de instancia), cambie los siguientes ajustes según sea necesario (amplíe Advanced Details (Detalles avanzados) para ver todos los ajustes) y, a continuación, elija Next: Add Storage (Siguiente: Añadir almacenamiento):

- Number of instances (Número de instancias): escriba el número de instancias que desea iniciar.

> **Tip**
>
> Para garantizar inicializacións de instancias más rápidos, divida las solicitudes de gran tamaño en lotes más pequeños. Por ejemplo, cree cinco solicitudes de inicialización independientes para 100 instancias cada una en lugar de una solicitud de inicialización para 500 instancias.

- (Opcional) Para ayudar a garantizar que se mantenga el número correcto de instancias para satisfacer la demanda de la aplicación, puede elegir Launch into Auto Scaling Group (iniciar en grupo de Auto Scaling) para crear una configuración de inicialización y un grupo de Auto Scaling. Auto Scaling escala el número de instancias en el grupo según sus especificaciones. Para obtener más información, consulte la Guía del usuario de Amazon EC2 Auto Scaling.

  > **Note**
  >
  > Si Amazon EC2 Auto Scaling marca una instancia que está en un grupo de escalado automático como incorrecta, la instancia se programará automáticamente para su reemplazo cuando se termine y se lance otra, y se pierden los datos de la instancia original. Una instancia se marca como incorrecta si detiene o reinicia la instancia o si otro evento marca la instancia como incorrecta. Para obtener más información, consulte Comprobaciones de estado de las instancias de escalado automático en la Guía del usuario de Amazon EC2 Auto Scaling.

- Purchasing option (Opción de compra): elija Request Spot instances (Solicitar instancias de spot) para iniciar una instancia spot. Esto añadirá y eliminará opciones de esta página. De manera opcional, puede establecer el precio máximo (no recomendado) y cambiar el tipo de solicitud, el comportamiento de interrupción y la validez de la solicitud. Para obtener más información, consulte Crear una solicitud de instancia de spot.
- Network (Red): seleccione la VPC o, para crear una VPC nueva, elija Create new VPC (Crear una VPC nueva) para ir a la consola de Amazon VPC. Cuando haya terminado, vuelva al asistente de inicialización de instancias y elija Refresh (Actualizar) para cargar su VPC en la lista.
- Subnet (Subred): puede iniciar una instancia en una subred asociada con una zona de disponibilidad, zona local, zona de Wavelength u Outpost.

  Para iniciar la instancia en una zona de disponibilidad, seleccione la subred en la que desea iniciar la instancia. Puede seleccionar No preference (Sin preferencia) para permitir que AWS elija una subred predeterminada en cualquier zona de disponibilidad. Para crear una subred, elija Create new subnet (Crear nueva subred) para ir a la consola de Amazon VPC. Cuando haya terminado, vuelva al asistente y elija Refresh (Actualizar) para cargar la subred en la lista.

  Para iniciar la instancia en una zona local, seleccione una subred que haya creado en la zona local.

  Para iniciar una instancia en un Outpost, seleccione una subred en una VPC que haya asociado a un Outpost.

- Auto-assign Public IP (Asignar IP pública automáticamente): especifique si la instancia recibe una dirección IPv4 pública. De forma predeterminada, las instancias en una subred predeterminada reciben una dirección IPv4 pública, mientras que las instancias en una subred no predeterminada no la reciben. Puede seleccionar Habilitar o Deshabilitar para anular la configuración predeterminada de la subred. Para obtener más información, consulte Direcciones IPv4 públicas.
- Auto-assign IPv6 IP (Asignar automáticamente IP IPv6): especifique si la instancia recibe una dirección IPv6 del rango de la subred. Seleccione Enable (Habilitar) o Disable (Deshabilitar) para anular la configuración predeterminada de la subred. Esta opción solo está disponible si ha asociado un bloque de CIDR IPv6 a la VPC y la subred. Para obtener más información, consulte Agregar bloques de CIDR IPv6 a una VPCen la Guía del usuario de Amazon VPC.
- Hostname type (Tipo de nombre de anfitrión): selecciónelo si desea que el nombre de host del sistema operativo invitado de la instancia incluya el nombre del recurso o el nombre de IP. Para obtener más información, consulte Tipos de nombres de host de instancias de Amazon EC2.
- DNS Hostname (Nombre de host DNS): determina si las consultas de DNS al nombre del recurso o de IP (según lo que haya seleccionado para Hostname type) responderán con la dirección IPv4 (registro A), dirección IPv6 (registro AAAA) o ambas. Para obtener más información, consulte Tipos de nombres de host de instancias de Amazon EC2.
- Directorio de unión al dominio: seleccione el directorio de AWS Directory Service (dominio) al que se ha unido la instancia después de la inicialización. Si selecciona un dominio, debe seleccionar un rol de IAM con los permisos necesarios. Para obtener más información sobre dominios que unen instancias de Linux, consulte Unir fácilmente una instancia de Linux EC2 a su directorio de Microsoft AD administrado de AWS. Para obtener más información acerca de dominios que unen instancias de Windows, consulte Cómo unir fácilmente una instancia EC2 de Windows.
- Placement group (Grupo de ubicación): un grupo de ubicación determina la estrategia de ubicación de las instancias. Seleccione un grupo de ubicación existente o cree uno nuevo. Esta opción solo está disponible si ha seleccionado un tipo de instancia que admita grupos de ubicación. Para obtener más información, consulte Grupos de ubicación.
- Reserva de capacidad: especifique si desea iniciar la instancia en capacidad compartida, cualquier Reserva de capacidad `open`, una Reserva de capacidad específica o un grupo de Reserva de capacidad. Para obtener más información, consulte iniciar instancias en una Reserva de capacidad existente.
- Rol de IAM: seleccione el rol de (IAM) AWS Identity and Access Management que desea asociar a la instancia. Para obtener más información, consulte Roles de IAM para Amazon EC2.

- CPU options (Opciones de CPU): elija Specify CPU options (Especificar opciones de CPU) para establecer un número personalizado de CPU virtuales durante la inicialización. Establezca el número de núcleos de la CPU y subprocesos por núcleo. Para obtener más información, consulte Optimización de las opciones de CPU.
- Shutdown behavior (Comportamiento de cierre): seleccione si la instancia debe detenerse o terminarse al cerrarla. Para obtener más información, consulte Cambiar el comportamiento de apagado iniciado por la instancia.
- Stop - Hibernate behavior (Detener - Comportamiento de hibernación): para habilitar la hibernación, seleccione esta casilla. Esta opción solo está disponible si la instancia satisface los requisitos previos de hibernación. Para obtener más información, consulte Hibernación de la instancia de Amazon EC2.
- Enable termination protection (Habilitar protección de terminación): seleccione esta casilla para evitar una terminación accidental. Para obtener más información, consulte Cómo habilitar la protección contra la terminación.
- Habilitar protección de detención: seleccione esta casilla de verificación para evitar una detención accidental. Para obtener más información, consulte Habilitación de la protección de detención.
- Monitoring (Supervisión): seleccione esta casilla para habilitar la supervisión detallada de su instancia con Amazon CloudWatch. Se aplican cargos adicionales. Para obtener más información, consulte Monitorear las instancias con CloudWatch.
- instancia optimizada para EBS: una instancia optimizada para Amazon EBS usa una pila de configuración optimizada y proporciona capacidad dedicada adicional para la E/S de Amazon EBS. Si el tipo de instancia admite esta característica, seleccione esta casilla de verificación para habilitarla. Se aplican cargos adicionales. Para obtener más información, consulte Instancias optimizadas para Amazon EBS.
- Tenancy (Tenencia): si va a iniciar la instancia en una VPC, puede elegir ejecutar la instancia en hardware dedicado y aislado (Dedicated [Dedicado]) o en un host dedicado (Dedicated host [Host dedicado]). Podrían aplicarse cargos adicionales. Para obtener más información, consulte Dedicated Instances y Dedicated Hosts.
- T2/T3 Unlimited: marque esta casilla para permitir ráfagas por encima de la base de referencia en las aplicaciones por el tiempo que sea necesario. Podrían aplicarse cargos adicionales. Para obtener más información, consulte Instancias de rendimiento ampliable.
- Sistemas de archivos: para crear un nuevo sistema de archivos para montarlo en la instancia, elija Crear nuevo sistema de archivos, ingrese un nombre para el nuevo sistema de archivos y, a continuación, elija Crear. El sistema de archivos se crea con Amazon EFS Creación rápida, que aplica la configuración recomendada por el servicio. Los grupos de seguridad necesarios para

habilitar el acceso al sistema de archivos se crean automáticamente y se asocian a la instancia y a los destinos de montaje del sistema de archivos. También puede elegir crear y adjuntar manualmente los grupos de seguridad necesarios. Para montar uno o varios sistemas de Amazon EFS archivos existentes en la instancia, elija Agregar sistema de archivos y, a continuación, elija los sistemas de archivos que desea montar y los puntos de montaje que desea utilizar. Para obtener más información, consulte Uso de Amazon EFS con instancias de Linux.

- Network interfaces (Interfaces de red): si seleccionó una subred específica, puede especificar hasta dos interfaces de red para la instancia:
  - En Network Interface (Interfaz de red), seleccione New network interface (Nueva interfaz de red) para que AWS cree una interfaz nueva o seleccione una interfaz de red existente disponible.
  - En Primary IP (IP principal), escriba una dirección IPv4 privada del rango de la subred o deje Auto-assign (Asignación automática) para que AWS elija una dirección IPv4 privada por usted.
  - En Secondary IP addresses (Direcciones IP secundarias), elija Add IP (Añadir IP) para asignar más de una dirección IPv4 privada a la interfaz de red seleccionada.
  - (Solo para IPv6) En IPv6 IPs (IP IPv6), elija Add IP (Agregar IP) e ingrese una dirección IPv6 del rango de la subred, o bien deje Auto-assign (Asignación automática) para que la elija AWS.
  - Índice de tarjeta de red: el índice de la tarjeta de red. La interfaz de red principal debe asignarse al índice 0 de la tarjeta de red. Algunos tipos de instancia admiten varias tarjetas de red.
  - Elija Add Device (Añadir dispositivo) para añadir una interfaz de red secundaria. Una interfaz de red secundaria puede residir en una subred distinta de la VPC, siempre que se encuentre en la misma zona de disponibilidad que la instancia.

  Para obtener más información, consulte Interfaces de red elásticas. Si especifica más de una interfaz de red, la instancia no puede recibir una dirección IPv4 pública. Además, si especifica una interfaz de red existente para eth0, no puede anular la configuración de la IPv4 pública de la subred con Auto-assign Public IP (Asignar IP pública automáticamente). Para obtener más información, consulte Asignar una dirección IPv4 pública durante la inicialización de la instancia.
- Kernel ID (ID de kernel): (solo válido para AMIs paravirtuales (PV)) seleccione Use default (Usar valor predeterminado) a menos que desee utilizar un kernel específico.
- RAM disk ID (ID de disco de RAM): (solo válido para AMIs paravirtuales (PV)) seleccione Use default (Usar valor predeterminado) a menos que desee utilizar un disco RAM específico. Si ha seleccionado un kernel, puede que tenga que seleccionar un disco RAM específico con los controladores necesarios.

- Enclave: seleccione Activar para habilitar la instancia de Nitro Enclaves de AWS. Para obtener más información, consulte ¿Qué son los Nitro Enclaves de AWS? en la Guía del usuario de Nitro Enclaves de AWS.
- Metadatos accesibles: puede habilitar o deshabilitar el acceso al servicio de metadatos de instancia (IMDS). Para obtener más información, consulte Utilizar IMDSv2.
- Punto de conexión IPv6 para la obtención de metadatos: puede permitir que una instancia utilice la dirección IPv6 del IMDS `[fd00:ec2::254]` para recuperar los metadatos de la instancia. Esta opción solo está disponible para el lanzamiento de instancias basadas en AWS Nitro System en una subred compatible con IPv6 (de doble pila o solo IPv6). Para obtener más información sobre cómo recuperar los metadatos de las instancias, consulte Recuperar metadatos de instancia.
- Versión de metadatos: si habilita el acceso a IMDS, puede optar por requerir el uso de la versión 2 del servicio de metadatos de instancia, al solicitar metadatos de instancia. Para obtener más información, consulte Configurar las opciones de metadatos para instancias nuevas.
- Límite de saltos para respuesta del token de metadatos: si habilita IMDS, puede establecer el número permitido de saltos de red para el token de metadatos. Para obtener más información, consulte Utilizar IMDSv2.
- User data (Datos de usuario): puede especificar los datos de usuario para configurar una instancia durante la inicialización o para ejecutar un script de configuración. Para adjuntar un archivo, seleccione la opción As file (Como archivo) y busque el archivo que desee adjuntar.

Paso 4: Agregar almacenamiento

La AMI que seleccione incluye uno o más volúmenes de almacenamiento, incluido el volumen de dispositivo raíz. En la página Add Storage (Añadir almacenamiento), puede especificar los volúmenes adicionales que desea adjuntar a la instancia eligiendo Add New Volume (Añadir nuevo volumen). Configure cada volumen como sigue y, a continuación, elija Next: Add Tags (Siguiente: Añadir etiquetas).

- Type (Tipo): seleccione el almacén de instancias o los volúmenes de Amazon EBS que desea asociar a la instancia. Los tipos de volumen disponibles en la lista dependen del tipo de instancia que haya elegido. Para obtener más información, consulte Almacén de instancias Amazon EC2 y Volúmenes de Amazon EBS.
- Device (Dispositivo): selecciónelo de la lista de nombres de dispositivo disponibles para el volumen.
- Snapshot (Instantánea): escriba el nombre o el ID de la instantánea desde la que desea restaurar un volumen. También puede buscar instantáneas públicas y compartidas disponibles escribiendo

texto en el campo Snapshot (Instantánea). Las descripciones de las instantáneas distinguen entre mayúsculas y minúsculas.

- Size (Tamaño): para volúmenes de EBS, puede especificar un tamaño de almacenamiento. Incluso si ha seleccionado una AMI y una instancia aptas para la capa gratuita, para permanecer en dicha capa debe mantenerse por debajo de los 30 GiB de almacenamiento total.
- Volume type (Tipo de volumen): elija un tipo de volumen para volúmenes de EBS. Para obtener más información, consulte Tipos de volúmenes de Amazon EBS en la Guía del usuario de Amazon EBS.
- IOPS: si ha seleccionado un tipo de volumen Provisioned IOPS SSD, puede ingresar el número de operaciones de E/S por segundo (IOPS) que puede soportar el volumen.
- Delete on Termination (Eliminar al terminar): para los volúmenes de Amazon EBS seleccione esta casilla para eliminar el volumen cuando se termine la instancia. Para obtener más información, consulte Conservación de los datos cuando se termina una instancia.
- Encrypted (Cifrado): si el tipo de instancia admite cifrado de EBS, puede especificar el estado de cifrado del volumen. Si ha habilitado el cifrado de forma predeterminada en esta región, se selecciona automáticamente la clave administrada por el cliente predeterminada. Puede seleccionar una clave diferente o deshabilitar el cifrado. Para obtener más información, consulte Cifrado de Amazon EBS en la Guía del usuario de Amazon EBS.

Paso 5: Añadir etiquetas

En la página Add Tags (Añadir etiquetas), especifique etiquetas proporcionando combinaciones de clave y valor. Puede etiquetar la instancia, los volúmenes o ambos. Para las instancias de spot, solo puede etiquetar la solicitud de instancia de spot. Elija Add another tag (Añadir otra etiqueta) para añadir más de una etiqueta a los recursos. Elija Next: Configure Security Group (Siguiente: Configurar grupo de seguridad) cuando haya terminado.

Paso 6: Configurar un grupo de seguridad

En la página Configure Security Group (Configurar grupo de seguridad), utilice un grupo de seguridad para definir reglas de firewall para la instancia. Estas reglas especifican qué tráfico procedente de la red se entregará en la instancia. El resto del tráfico se ignora. (Para obtener más información acerca de los grupos de seguridad, consulte Grupos de seguridad de Amazon EC2 para instancias EC2.) Seleccione o cree un grupo de seguridad como se indica a continuación y, a continuación, elija Review and Launch (Revisar y iniciar).

- Para seleccionar un grupo de seguridad existente, hágalo desde la opción Select an existing security group (Seleccionar un grupo de seguridad existente). Las reglas de un grupo de seguridad existente no se pueden editar, pero puede copiarlas en un grupo nuevo eligiendo Copy to new (Copiar en uno nuevo). Entonces podrá añadir reglas como se describe en el paso siguiente.
- Para crear un grupo de seguridad, elija Create a new security group (Crear un grupo de seguridad nuevo). El asistente define automáticamente el grupo de seguridad launch-wizard-x crea una regla de entrada para que pueda conectarse a la instancia. Las instancias de Linux usan una regla de entrada para SSH (puerto 22) y las instancias de Windows usan una regla de entrada para RDP (puerto 3389).
- Puede añadir reglas para adaptarse a sus necesidades. Por ejemplo, si la instancia es un servidor web, abra los puertos 80 (HTTP) y 443 (HTTPS) para permitir el tráfico de Internet.

  Para añadir una regla, elija Add Rule (Añadir regla), seleccione el protocolo para abrir el tráfico de la red y, a continuación, especifique el origen. Elija My IP (Mi IP) en la lista Source (Origen) para que asistente añada las direcciones IP públicas de su equipo. Sin embargo, si se conecta a través de un ISP o protegido por su firewall sin una dirección IP estática, deberá encontrar el rango de direcciones IP utilizadas por los equipos cliente.

  > **Warning**
  >
  > Las reglas que permiten a todas las direcciones IP (`0.0.0.0/0`) acceder a su instancia por SSH or RDP son aceptables para este rápido ejercicio, pero no son seguras para entornos de producción. Debe autorizar el acceso a su instancia únicamente a una dirección IP o a un rango de direcciones IP específico.

Paso 7: Revisar la inicialización de la instancia y seleccionar el par de claves

En la página Review Instance Launch (Revisar inicialización de instancia), compruebe los detalles de la instancia y haga los cambios necesarios seleccionando el enlace Edit (Editar) correspondiente.

Cuando esté preparado, elija Launch (iniciar).

En el cuadro de diálogo Select an existing key pair or create a new key pair (Seleccionar par de claves existentes o crear nuevo par de claves), puede elegir un par de claves existente o crear uno nuevo. Por ejemplo, elija Choose an existing key pair (Elegir un par de claves existente) y, a continuación, seleccione el par de claves que creó al obtener la configuración. Para obtener más información, consulte Pares de claves e instancias de Amazon EC2.

> **Important**
>
> Si elige la opción Proceed without key pair (Continuar sin un par de claves), no podrá conectarse a la instancia a menos que elija una AMI que esté configurada para ofrecer a los usuarios otra forma de iniciar sesión.

Para iniciar la instancia, active la casilla de verificación de confirmación y, a continuación, elija Launch Instances (iniciar instancias).

(Opcional) Puede crear una alarma de comprobación de estado para la instancia (podrían aplicarse tarifas adicionales). En la pantalla de confirmación, elija Create status check alarms (Crear alarmas de comprobación de estado) y siga las instrucciones. Las alarmas de comprobación de estado también se pueden crear después de iniciar la instancia. Para obtener más información, consulte Crear y editar alarmas de comprobación de estado.

Si se produce un error al iniciar la instancia o el estado pasa inmediatamente a `terminated` en lugar de `running`, consulte Solucionar problemas de lanzamiento de instancias.

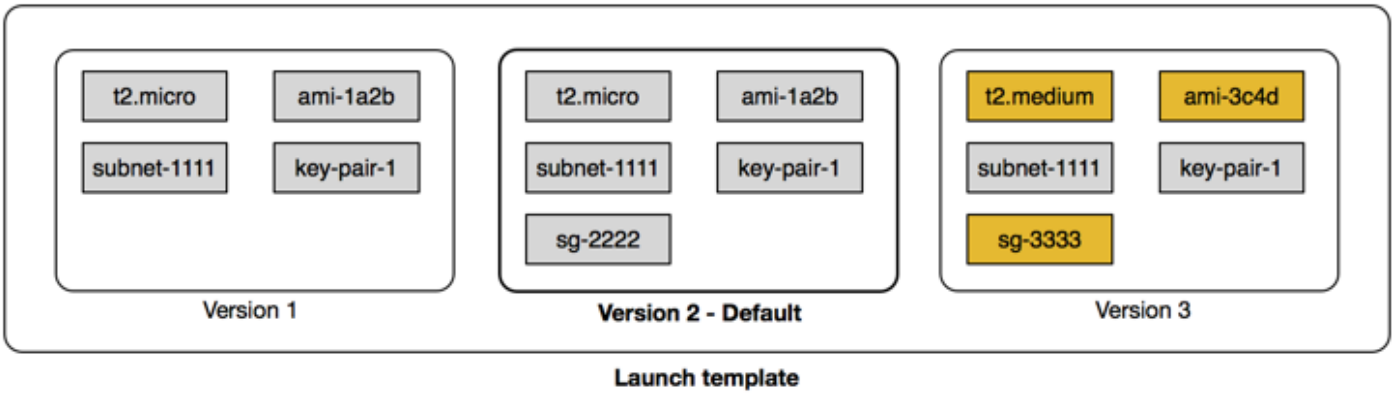
iniciar una instancia desde una plantilla de inicialización

Puede utilizar una plantilla de inicialización para almacenar parámetros de inicialización de instancias con el objetivo de no tener que especificarlos cada vez que lance una. Por ejemplo, puede crear una plantilla de inicialización con el ID de la AMI, el tipo de instancia y la configuración de red que suele usar para iniciar instancias. Al iniciar una instancia mediante la consola de Amazon EC2, un SDK de AWS o una herramienta de la línea de comandos, puede especificar la plantilla de inicialización en lugar de volver a ingresar los parámetros.

Para cada plantilla de inicialización, puede crear una o varias versiones de plantillas de inicialización numeradas. Cada versión tiene diferentes parámetros de inicialización. Al iniciar una instancia desde una plantilla de inicialización, puede utilizar cualquier versión de la plantilla. Si no especifica una versión, se usa la predeterminada. Puede definir cualquier versión de la plantilla de inicialización como predeterminada — la versión predeterminada es la primera.

En el siguiente diagrama se muestra la plantilla de inicialización con tres versiones. La primera versión especifica el tipo de instancia, el ID de la AMI, la subred y el par de claves que utilizar para iniciar la instancia. La segunda versión se basa en la primera y también especifica un grupo de seguridad de la instancia. La tercera versión usa distintos valores para algunos de los parámetros.

La versión 2 se establece como la predeterminada. Si ha iniciado la instancia desde esta plantilla de inicialización, se usarían los parámetros de la versión 2 si no se especificara ninguna otra versión.



Contenido

- Restricciones de las plantillas de inicialización
- Controle el acceso a las plantillas de inicialización con permisos de IAM
- Utilice plantillas de inicialización para controlar la inicialización de instancias
- Creación de una plantilla de lanzamiento
- Modificar una plantilla de inicialización (administrar versiones de plantillas de inicialización)
- Eliminación de una plantilla de inicialización
- iniciar instancias desde una plantilla de inicialización

Restricciones de las plantillas de inicialización

Las siguientes reglas se aplican a las plantillas de inicialización y a las versiones:

- Cuotas: para ver las cuotas de las plantillas de inicialización y las versiones de las plantillas de inicialización, abra la consola de Service Quotas o utilice el comando de la AWS CLI list-service-quotas. Cada cuenta de AWS puede tener un máximo de 5000 plantillas de inicialización por región y hasta 10 000 versiones por plantilla de inicialización. Es posible que sus cuentas tengan cuotas diferentes en función de su antigüedad e historial de uso.
- Los parámetros son opcionales: los parámetros de la plantilla de inicialización son opcionales. Sin embargo, debe asegurarse de que la solicitud para iniciar una instancia incluya todos los parámetros necesarios. Por ejemplo, si su plantilla de inicialización no incluye una ID de AMI, debe especificar la plantilla de inicialización y una ID de AMI al iniciar una instancia.

- Parámetros no validados: los parámetros de la plantilla de inicialización no están completamente validados cuando crea dicha plantilla. Si especifica valores incorrectos para parámetros, o si no utiliza combinaciones de parámetros compatibles, no se puede iniciar ninguna instancia con esta plantilla de inicialización. Asegúrese de especificar los valores de parámetros correctos y de estar usando combinaciones de parámetros admitidas. Por ejemplo, para iniciar una instancia en un grupo de ubicación, debe especificar un tipo de instancia admitido.
- Etiquetas: puede etiquetar plantillas de inicialización, pero no puede etiquetar sus versiones.
- Inmutable: las plantillas de inicialización son inmutables. Para modificar una plantilla de inicialización, debe crear una nueva versión de la plantilla de inicialización.
- Números de versión: las versiones de las plantillas de inicialización están numeradas en el orden en el que se han creado. Al crear una versión de una plantilla de inicialización, no puede especificar el número de versión.

Controle el acceso a las plantillas de inicialización con permisos de IAM

Puede utilizar los permisos de IAM para controlar qué acciones de la plantilla de inicialización pueden realizar los usuarios, como ver, crear o eliminar plantillas de inicialización.

Cuando se concede permiso a los usuarios para crear plantillas de inicialización y versiones de las mismas, no se pueden utilizar los permisos de nivel de recursos para restringir los recursos que pueden especificar en una plantilla de inicialización. Por lo tanto, asegúrese de conceder permisos para crear plantillas de inicialización y versiones de plantillas de inicialización sólo a los administradores apropiados.

Debe conceder a cualquier persona que vaya a utilizar una plantilla de inicialización los permisos necesarios para crear y acceder a los recursos especificados en la plantilla de inicialización. Por ejemplo:

- Para inicializar una instancia desde una Imagen de máquina de Amazon (AMI) privada compartida, el usuario debe tener permiso de inicialización para la AMI.
- Para crear volúmenes de EBS con etiquetas de instantáneas existentes, el usuario debe tener acceso de lectura a las instantáneas y permisos para crear y etiquetar volúmenes.

Contenido

- ec2:DescribeLaunchTemplateVersions
- ec2:DeleteLaunchTemplate
- Controle los permisos del control de versiones
- Controle el acceso a las etiquetas de las plantillas de inicialización

ec2:CreateLaunchTemplate

Para crear una plantilla de inicialización en la consola o mediante las API, la entidad principal debe tener el permiso `ec2:CreateLaunchTemplate` en una política de IAM. Siempre que sea posible, utilice etiquetas que le ayuden a controlar el acceso a las plantillas de inicialización de su cuenta.

Por ejemplo, la siguiente declaración de política de IAM otorga a la entidad principal permiso para crear plantillas de inicialización solo si la plantilla usa la etiqueta especificada (*purpose*=*testing*).

```
{
    "Sid": "IAMPolicyForCreatingTaggedLaunchTemplates",
    "Action": "ec2:CreateLaunchTemplate",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/purpose": "testing"
        }
    }
}
```

Es posible que las entidades principales que crean claves necesiten algunos permisos relacionados.

- ec2:CreateTags: para añadir etiquetas a la plantilla de inicialización durante la operación `CreateLaunchTemplate`, la persona que llama `CreateLaunchTemplate` debe tener el permiso `ec2:CreateTags` en una política de IAM.
- ec2:RunInstances: para iniciar instancias de EC2 a partir de la plantilla de inicialización que crearon, la entidad principal también debe tener el permiso `ec2:RunInstances` en una política de IAM.

En las acciones de creación de recursos que aplican etiquetas, los usuarios deben tener el permiso `ec2:CreateTags`. La siguiente instrucción de política de IAM utiliza la clave de condición `ec2:CreateAction` para permitir a los usuarios crear etiquetas únicamente en el contexto de

`CreateLaunchTemplate`. Los usuarios no pueden etiquetar plantillas de inicialización que ya existan ni otros recursos. Para obtener más información, consulte Conceder permisos para etiquetar recursos durante la creación.

```
{
    "Sid": "IAMPolicyForTaggingLaunchTemplatesOnCreation",
    "Action": "ec2:CreateTags",
    "Effect": "Allow",
    "Resource": "arn:aws:ec2:region:account-id:launch-template/*",
    "Condition": {
        "StringEquals": {
            "ec2:CreateAction": "CreateLaunchTemplate"
        }
    }
}
```

El usuario de IAM que crea una plantilla de inicialización no tiene automáticamente permiso para usar la plantilla de inicialización que ha creado. Al igual que cualquier otra entidad principal, el creador de la clave necesita obtener permiso a través de una política de IAM. Si un usuario de IAM quiere iniciar una instancia de EC2 a partir de una plantilla de inicialización, debe tener el permiso `ec2:RunInstances`. Al conceder estos permisos, puede especificar que los usuarios solo puedan usar plantillas de inicialización con etiquetas o ID específicos. También puede controlar la AMI y otros recursos a los que cualquier persona que utilice plantillas de inicialización puede hacer referencia y utilizar al iniciar instancias especificando los permisos a nivel de recursos para la llamada `RunInstances`. Para ver ejemplos de políticas, consulte Plantillas de lanzamiento.

ec2:DescribeLaunchTemplates

Para enumerar las plantillas de inicialización de la cuenta, la entidad principal debe tener el permiso `ec2:DescribeLaunchTemplates` en una política de IAM. Puesto que las acciones `Describe` no admiten permisos a nivel de recurso, debe especificarlos sin condiciones y el valor del elemento de recurso en la política debe ser `"*"`.

Por ejemplo, la siguiente declaración de política de IAM otorga el permiso a la entidad principal para enumerar todas las plantillas de inicialización en la cuenta.

```
{
    "Sid": "IAMPolicyForDescribingLaunchTemplates",
    "Action": "ec2:DescribeLaunchTemplates",
    "Effect": "Allow",
```

```
    "Resource": "*"
}
```

ec2:DescribeLaunchTemplateVersions

Las entidades principales que consulten las plantillas de inicialización también deberían tener el permiso `ec2:DescribeLaunchTemplateVersions` para recuperar todo el conjunto de atributos que componen las plantillas de inicialización.

Para enumerar las versiones de las plantillas de inicialización de la cuenta, la entidad principal debe tener el permiso `ec2:DescribeLaunchTemplateVersions` en una política de IAM. Puesto que las acciones `Describe` no admiten permisos a nivel de recurso, debe especificarlos sin condiciones y el valor del elemento de recurso en la política debe ser `"*"`.

Por ejemplo, la siguiente declaración de política de IAM otorga el permiso a la entidad principal para enumerar todas las versiones de las plantillas de inicialización en la cuenta.

```
{
    "Sid": "IAMPolicyForDescribingLaunchTemplateVersions",
    "Effect": "Allow",
    "Action": "ec2:DescribeLaunchTemplateVersions",
    "Resource": "*"
}
```

ec2:DeleteLaunchTemplate

> **Important**
>
> Debe tener precaución al dar permiso a las entidades principales para eliminar un recurso. Eliminar una plantilla de inicialización puede provocar un error en un recurso de AWS que se base en la plantilla de inicialización.

Para eliminar una plantilla de inicialización, la entidad principal debe tener el permiso `ec2:DeleteLaunchTemplate` en una política de IAM. Siempre que sea posible, use claves de condición basadas en etiquetas para limitar los permisos.

Por ejemplo, la siguiente declaración de política de IAM otorga a la entidad principal permiso para eliminar plantillas de inicialización solo si la plantilla usa la etiqueta especificada (*purpose*=*testing*).

```
{
    "Sid": "IAMPolicyForDeletingLaunchTemplates",
    "Action": "ec2:DeleteLaunchTemplate",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/purpose": "testing"
        }
    }
}
```

Como alternativa, puede utilizar los ARN para identificar la plantilla de inicialización a la que se aplica la política de IAM.

Una plantilla de inicialización tiene el siguiente ARN.

```
"Resource": "arn:aws:ec2:region:account-id:launch-template/lt-09477bcd97b0d310e"
```

Puede especificar varios ARN incluyéndolos en una lista o puede especificar un valor `Resource` de `"*"` sin el elemento `Condition` para que la entidad principal pueda eliminar cualquier plantilla de inicialización de la cuenta.

Controle los permisos del control de versiones

Los administradores de confianza pueden conceder acceso para crear y eliminar versiones de una plantilla de inicialización y para cambiar la versión predeterminada de una plantilla de inicialización mediante políticas de IAM similares a las de los ejemplos siguientes.

> **Important**
>
> Tenga cuidado al dar permiso a las entidades principales para crear versiones de plantillas de inicialización o modificar las plantillas de inicialización.
>
> - Cuando crea una versión de la plantilla de inicialización, afecta a cualquier recurso de AWS que permite a Amazon EC2 iniciar instancias en su nombre con la versión `Latest`.
> - Cuando modifica una versión de la plantilla de inicialización, puede cambiar qué versión es el `Default` y por lo tanto afectar los recursos de AWS que permite a Amazon EC2 iniciar instancias en su nombre con esta versión modificada.

También debe ser cauteloso a la hora de gestionar los recursos de AWS que interactúan con la versión de plantilla de inicialización `Latest` o `Default`, como la flota de EC2 y la flota de spot. Cuando se utiliza una versión diferente de la plantilla de inicialización para `Latest` o `Default`, Amazon EC2 no vuelve a comprobar los permisos para completar las acciones al iniciar nuevas instancias a fin de cumplir con la capacidad de destino de la flota porque no hay interacción del usuario con el recurso de AWS. Al conceder permiso a un usuario para llamar a las API de `CreateLaunchTemplateVersion` y `ModifyLaunchTemplate`, el usuario también obtiene el permiso `iam:PassRole` si dirige la flota a una versión de plantilla de inicialización diferente que contenga un perfil de instancia (un contenedor para un rol de IAM). Esto significa que un usuario puede actualizar una plantilla de inicialización para transferir un rol de IAM a una instancia, incluso si no tiene el permiso `iam:PassRole`. Para gestionar este riesgo, tenga cuidado al conceder permisos a las personas que pueden crear y gestionar las versiones de las plantillas de inicialización.

ec2:CreateLaunchTemplateVersion

Para crear una nueva versión de una plantilla de inicialización, la entidad principal debe tener el permiso `ec2:CreateLaunchTemplateVersion` para la plantilla de inicialización en una política de IAM.

Por ejemplo, la siguiente declaración de política de IAM otorga a la entidad principal permiso para crear las versiones de plantillas de inicialización solo si la versión usa la etiqueta especificada (*`environment`*=*`production`*). Como alternativa, puede especificar uno o varios ARN de plantilla de inicialización, o puede especificar un valor `Resource` de `"*"` sin el elemento `Condition` que permite a la entidad principal crear versiones de cualquier plantilla de inicialización de la cuenta.

```
{
    "Sid": "IAMPolicyForCreatingLaunchTemplateVersions",
    "Action": "ec2:CreateLaunchTemplateVersion",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/environment": "production"
        }
    }
}
```

ec2:DeleteLaunchTemplateVersion

> **Important**
>
> Como siempre, debe tener precaución al dar permiso a las entidades principales para eliminar un recurso. Eliminar una versión de plantilla de inicialización puede provocar un error en un recurso de AWS que se base en la versión de plantilla de inicialización.

Para eliminar una versión de una plantilla de inicialización, la entidad principal debe tener el permiso `ec2:DeleteLaunchTemplateVersion` para la plantilla de inicialización en una política de IAM.

Por ejemplo, la siguiente declaración de política de IAM otorga a la entidad principal permiso para eliminar las versiones de plantillas de inicialización solo si la versión usa la etiqueta especificada (*`environment`*=*`production`*). Como alternativa, puede especificar uno o varios ARN de plantilla de inicialización, o puede especificar un valor `Resource` de `"*"` sin el elemento `Condition` que permite a la entidad principal eliminar versiones de cualquier plantilla de inicialización de la cuenta.

```
{
    "Sid": "IAMPolicyForDeletingLaunchTemplateVersions",
    "Action": "ec2:DeleteLaunchTemplateVersion",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/environment": "production"
        }
    }
}
```

ec2:ModifyLaunchTemplate

Para cambiar la versión `Default` asociada a una plantilla de inicialización, la entidad principal debe tener el permiso `ec2:ModifyLaunchTemplate` para la plantilla de inicialización en una política de IAM.

Por ejemplo, la siguiente declaración de política de IAM otorga a la entidad principal permiso para modificar plantillas de inicialización solo si la plantilla de inicialización usa la etiqueta especificada (*`environment`*=*`production`*). Como alternativa, puede especificar uno o varios ARN de plantilla

de inicialización, o puede especificar un valor `Resource` de `"*"` sin el elemento `Condition` que permite a la entidad principal modificar cualquier plantilla de inicialización de la cuenta.

```
{
    "Sid": "IAMPolicyForModifyingLaunchTemplates",
    "Action": "ec2:ModifyLaunchTemplate",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/environment": "production"
        }
    }
}
```

Controle el acceso a las etiquetas de las plantillas de inicialización

Puede utilizar claves de condición para limitar los permisos de etiquetado cuando el recurso es una plantilla de inicialización. Por ejemplo, la siguiente política de IAM permite eliminar solo la etiqueta con la clave *temporary* de las plantillas de inicialización de la cuenta y región especificadas.

```
{
    "Sid": "IAMPolicyForDeletingTagsOnLaunchTemplates",
    "Action": "ec2:DeleteTags",
    "Effect": "Allow",
    "Resource": "arn:aws:ec2:region:account-id:launch-template/*",
    "Condition": {
        "ForAllValues:StringEquals": {
            "aws:TagKeys": ["temporary"]
        }
    }
}
```

Para obtener más información sobre las condiciones, claves que puede utilizar para controlar las etiquetas, y las claves y los valores que se pueden aplicar a los recursos de Amazon EC2, consulte Controlar el acceso a etiquetas específicas.

Utilice plantillas de inicialización para controlar la inicialización de instancias

Puede especificar que los usuarios puedan iniciar instancias únicamente si usan una plantilla de inicialización y que solo puedan usar una plantilla de inicialización específica. También puede

controlar quién puede crear, modificar, describir y eliminar plantillas de inicialización y versiones de las mismas.

Usar plantillas de inicialización para controlar los parámetros de inicialización

Una plantilla de inicialización puede contener algunos o todos los parámetros necesarios para iniciar una instancia. Al iniciar una instancia con una plantilla de inicialización, puede reemplazar parámetros especificados en dicha plantilla. También puede especificar parámetros adicionales que no están en la plantilla de inicialización.

> **Note**
>
> Durante la inicialización, no es posible eliminar parámetros de plantillas de inicialización (por ejemplo, no puede especificar un valor “null” en el parámetro). Para eliminar un parámetro, cree una nueva versión de la plantilla de inicialización sin el parámetro y úsela para iniciar la instancia.

Para iniciar instancias, los usuarios deben tener permisos de uso para la acción `ec2:RunInstances`. Los usuarios también deben disponer de permisos para crear o utilizar los recursos creados con la instancia o asociados a ella. Puede utilizar permisos de nivel de recurso para la acción `ec2:RunInstances` para controlar los parámetros de inicialización que pueden especificar los usuarios. También puede conceder permisos a los usuarios para iniciar una instancia con una plantilla de inicialización. Esto le permite administrar parámetros de inicialización en una plantilla de inicialización en lugar de en una política de IAM y usar una plantilla de inicialización como vehículo de autorización para iniciar instancias. Por ejemplo, puede especificar que los usuarios pueden iniciar instancias únicamente mediante una plantilla de inicialización y que solo deben usar una plantilla de inicialización específica. También puede controlar los parámetros de inicialización que los usuarios pueden omitir en la plantilla de inicialización. Para ver ejemplos de políticas, consulte Plantillas de lanzamiento.

Controlar el uso de las plantillas de inicialización

De forma predeterminada, los usuarios no tienen permisos para trabajar con plantillas de inicialización. Puede crear una política que conceda a los usuarios permisos para crear, modificar, describir y eliminar plantillas de inicialización y versiones de plantillas de inicialización. También puede aplicar permisos de nivel de recursos a algunas acciones de plantillas de inicialización para controlar la capacidad de un usuario de emplear recursos específicos en esas acciones. Para

obtener más información, consulte los siguientes ejemplos de políticas: Ejemplo: Trabajar con plantillas de lanzamiento

Sea precavido a la hora de conceder permisos a los usuarios para utilizar las acciones `ec2:CreateLaunchTemplate` y `ec2:CreateLaunchTemplateVersion`. No puede usar los permisos de nivel de recursos para controlar qué recursos pueden especificar los usuarios en la plantilla de inicialización. Para restringir los recursos que se usan para iniciar una instancia, asegúrese de conceder permisos para crear plantillas de inicialización y versiones de las mismas solo a los administradores adecuados.

Problemas de seguridad importantes al utilizar plantillas de inicialización con flota de EC2 o Flota de spot

Para usar plantillas de inicialización, debe conceder permisos a los usuarios para crear, modificar, describir y eliminar plantillas de inicialización y versiones de plantillas de inicialización. Puede controlar quién puede crear plantillas de inicialización y iniciar versiones de plantillas al controlar el acceso a las acciones `ec2:CreateLaunchTemplate` y `ec2:CreateLaunchTemplateVersion`. También puede controlar el acceso a la acción `ec2:ModifyLaunchTemplate` para controlar quién puede modificar las plantillas de inicialización.

> **Important**
>
> Si una flota de EC2 o Flota de spot está configurada para utilizar la versión de la plantilla de inicialización más reciente o predeterminada, la flota no sabrá si la más reciente o la predeterminada se modificaron posteriormente para que apunten a una versión diferente de la plantilla de inicialización. Cuando se utiliza una versión diferente de la plantilla de inicialización para la versión más reciente o la predeterminada, Amazon EC2 no vuelve a comprobar los permisos para completar las acciones al iniciar nuevas instancias a fin de cumplir con la capacidad de destino de la flota. Esta es una consideración importante al conceder permisos a quién puede crear y administrar las versiones de la plantilla de inicialización; en particular, la acción `ec2:ModifyLaunchTemplate` que permite al usuario cambiar la versión de la plantilla de inicialización predeterminada.

Al conceder permiso a un usuario para utilizar las acciones de EC2 para las API de la plantilla de inicialización, también se concede el permiso `iam:PassRole` al usuario si crea o actualiza una flota de EC2 o una Flota de spot para que apunte a una versión diferente de la plantilla de inicialización que contenga un perfil de instancia (un contenedor para un rol de IAM). Esto significa que un usuario

puede actualizar una plantilla de inicialización para transferir un rol de IAM a una instancia, incluso si no tiene el permiso `iam:PassRole`. Para obtener más información y una política de IAM de ejemplo, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias de Amazon EC2 en la Guía del usuario de IAM.

Para obtener más información, consulte Controlar el uso de las plantillas de inicialización y Ejemplo: Trabajar con plantillas de lanzamiento.

Creación de una plantilla de lanzamiento

Cree una nueva plantilla de inicialización con los parámetros que defina, o utilice una plantilla de inicialización o una instancia como base para la nueva plantilla de inicialización.

Tareas

- Creación de una plantilla de inicialización a partir de parámetros
- Crear una plantilla de inicialización a partir de una existente
- Crear una plantilla de inicialización a partir de una instancia
- Uso de un parámetro de Systems Manager en lugar de un ID de AMI

Creación de una plantilla de inicialización a partir de parámetros

Para crear una plantilla de inicialización, debe especificar el nombre y al menos un parámetro de configuración de instancia.

Direcciones de consola

Cómo crear una versión de una plantilla de inicialización mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Launch Templates (Plantillas de inicialización) y, a continuación, Create launch template (Crear plantilla de inicialización).
3. Los parámetros de la plantilla de inicialización están agrupados. Para obtener detalles acerca de cada grupo, consulte las siguientes secciones.
4. Utilice el panel Resumen para revisar la configuración de la plantilla de inicialización. Puede ir a cualquier sección seleccionando su enlace y, a continuación, realizar los cambios necesarios.
5. Cuando esté listo para crear su plantilla de inicialización, elija Create launch template (Crear plantilla de inicialización).

Nombre, descripción y etiquetas de la plantilla de inicialización

1. En Nombre de plantilla de inicialización, introduzca un nombre descriptivo para la plantilla.
2. En Template version description (Descripción de la versión de plantilla), ingrese una breve descripción para esta versión de la plantilla de inicialización.
3. Para etiquetar la plantilla de inicialización durante la creación, expanda Template tags (Etiquetas de plantilla), elija Add Tag (Agregar etiqueta) y, a continuación, introduzca un par de clave y valor de etiqueta. Elija Add tag (Agregar etiqueta) para cada etiqueta adicional.

> **Note**
>
> Para etiquetar los recursos que se crean cuando se inicia una instancia, debe especificar las etiquetas en Resource tags (Etiquetas de recursos). Para obtener más información, consulte Etiquetas de recursos.

Imágenes de aplicaciones y sistema operativo (Imagen de máquina de Amazon)

Una Imagen de máquina de Amazon (AMI) proporciona la información necesaria para crear una instancia. Por ejemplo, una AMI puede contener el software necesario para funcionar como servidor web, como Linux, Apache y su sitio web.

Puede encontrar una AMI adecuada de la siguiente manera: Con cada opción para buscar una AMI, puede elegir Cancel (Cancelar) (en la parte superior derecha) para volver a la plantilla de inicialización sin elegir una AMI.

Barra de búsqueda

Para buscar en todas las AMI disponibles, ingrese una palabra clave en la barra de búsqueda de AMI y pulse Enter (Intro). Elija Select (Seleccionar) para seleccionar una AMI.

Recents (Recientes)

Las AMI que se han usado recientemente.

Elija iniciada recientemente o Actualmente en uso y, a continuación, desde Imagen de máquina de Amazon (AMI), seleccione una AMI.

Mis AMI

Las AMI privadas de su propiedad o las AMI privadas que se han compartido con usted.

Elija De mi propiedad o Compartido conmigo y, a continuación, desde Imagen de máquina de Amazon (AMI), seleccione una AMI.

Quick Start (Inicio rápido)

Las AMI están agrupadas por sistema operativo (SO) para ayudar a comenzar rápidamente a trabajar.

En primer lugar, seleccione el sistema operativo que necesita y, a continuación, en Imagen de máquina de Amazon (AMI), seleccione una AMI. Para seleccionar una AMI que sea apta para nivel gratuito, asegúrese de que la AMI esté marcada como Free tier eligible (Apta para nivel gratuito).

Browse more AMIs (Examinar más AMI)

Elija Browse more AMIs (Examinar más AMI) para navegar por el catálogo completo de AMI.

- Para buscar en todas las AMI disponibles, escriba una palabra clave en la barra de búsqueda y pulse Intro.
- Para buscar una AMI mediante un parámetro de Systems Manager, elija el botón de flecha situado a la derecha de la barra de búsqueda y luego elija Search by Systems Manager parameter (Buscar por parámetro de Systems Manager). Para obtener más información, consulte Cómo buscar una AMI con un parámetro de Systems Manager.
- Para especificar un parámetro de Systems Manager que se resolverá en una AMI en el momento en que se lance una instancia desde la plantilla de inicialización, elija el botón de flecha situado a la derecha de la barra de búsqueda y luego elija Especificar valor personalizado/parámetro de Systems Manager. Para obtener más información, consulte Uso de un parámetro de Systems Manager en lugar de un ID de AMI.
- Para buscar por categoría, elija Quickstart AMIs (AMI de inicio rápido), My AMIs (Mis AMI), AWS Marketplace AMIs (AMI) o Community AMIs (AMI de comunidad).

  AWS Marketplace es una tienda en línea donde puede comprar el software que se ejecuta en AWS, incluidas las AMI. Para obtener más información sobre cómo iniciar una instancia desde AWS Marketplace, consulte iniciar una AWS Marketplace instancia. En Community AMIs (AMI de comunidad), puede encontrar las AMI que los miembros de la comunidad de AWS han puesto a disposición de los demás. Las AMI de Amazon o de un socio verificado están marcadas como Verified provider (Proveedor verificado).
- Para filtrar la lista de AMI, active una o varias casillas de verificación en Refine results (Refinar los resultados) a la izquierda de la pantalla. Las opciones de filtro son diferentes en función de la categoría de búsqueda seleccionada.

- Compruebe la lista Tipo de dispositivo raíz que se muestra para cada AMI. Observe cuáles son las AMI del tipo que necesita, ebs (respaldadas por Amazon EBS) o bien instance-store (con respaldo en el almacén de instancias). Para obtener más información, consulte Almacenamiento para el dispositivo raíz.
- Compruebe la lista Tipo de virtualización que se muestra para cada AMI. Observe cuáles son las AMI del tipo que necesita, hvm o paravirtual. Por ejemplo, algunos tipos de instancias requieren una HVM. Para obtener más información, consulte Tipos de virtualización de AMI.
- Compruebe el modo de arranque que aparece para cada AMI. Observe qué AMI utiliza el modo de arranque que necesita: legacy-bios, uefi o uefi-preferred. Para obtener más información, consulte Modos de arranque de Amazon EC2.
- Elija una AMI que satisfaga sus necesidades y, a continuación, elija Seleccionar.

Tipo de instancia

El tipo de instancia define la configuración de hardware y el tamaño de la instancia. Los tipos de instancia más grandes tienen una CPU y memoria superiores. Para obtener más información, consulte Tipos de instancias de Amazon EC2.

En Tipo de instancia, puede seleccionar un tipo de instancia o especificar atributos de instancia y permitir que Amazon EC2 identifique los tipos de instancia con esos atributos.

> **Note**
>
> La especificación de atributos de instancia solo se admite cuando se utilizan grupos de escalado automático, flotas de EC2 y flotas de spot para iniciar instancias. Para obtener más información, consulte Creación de un grupo de Auto Scaling mediante la selección de tipo de instancia basada en atributos, Selección de tipo de instancia basada en atributos para la flota de EC2 y Selección de tipo de instancia basada en atributos para la flota de spot.
> Si planea utilizar la plantilla de inicialización en el asistente de instancias de inicialización o con la API RunInstances, debe seleccionar un tipo de instancia.

- Instance type (Tipo de instancia): asegúrese de que el tipo de instancia sea compatible con la AMI que ha especificado. Para obtener más información, consulte Tipos de instancias de Amazon EC2.
- Comparación de tipos de instancia: puede comparar distintos tipos de instancia mediante los siguientes atributos: número de vCPU, arquitectura, cantidad de memoria (GiB), cantidad de almacenamiento (GB), tipo de almacenamiento y rendimiento de red.

- Obtener asesoramiento: puede obtener orientación y sugerencias sobre tipos de instancias en el selector de tipos de instancias de EC2 de Amazon Q. Para obtener más información, consulte Obtención de recomendaciones de tipos de instancias para una nueva carga de trabajo.
- Avanzado: para especificar los atributos de instancia y permitir que Amazon EC2 identifique los tipos de instancias con esos atributos, elija Avanzado y luego seleccione Especificar atributos de tipo de instancia.
  - Number of vCPUs (Número de vCPU): ingrese el número mínimo y máximo de vCPU para los requisitos de computación. Para indicar que no hay límites, ingrese un mínimo de **0** y deje el máximo en blanco.
  - Amount of memory (MiB) (Cantidad de memoria [MiB]): ingrese la cantidad mínima y máxima de memoria, en MiB, para los requisitos de computación. Para indicar que no hay límites, ingrese un mínimo de **0** y deje el máximo en blanco.
  - Expanda Optional instance type attributes (Atributos de tipo de instancia opcionales) y elija Add attribute (Agregar atributo) para expresar sus requisitos de computación con más detalle. Para obtener más información acerca de cada atributo, consulte InstanceRequirementsRequest en la Referencia de la API de Amazon EC2.
  - Resulting instance types (Tipos de instancia resultantes): puede obtener una vista previa de los tipos de instancia que coinciden con los atributos especificados. Para excluir tipos de instancia, elija Add attribute (Agregar atributo) y, desde la lista Attribute (Atributo), elija Excluded instance types (Tipos de instancia excluidos). De la lista Attribute Value (Valor de atributo), seleccione los tipos de instancia que desea excluir.

Par de claves (inicio de sesión)

El par de claves para la instancia.

En Key pair name (Nombre de par de claves) seleccione un par de claves existente o seleccione Create new key pair (Crear nuevo par de claves) para crear uno nuevo. Para obtener más información, consulte Pares de claves e instancias de Amazon EC2.

Network settings (Configuración de red)

Establezca la configuración de red, según sea necesario.

- Subnet (Subred): puede iniciar una instancia en una subred asociada con una zona de disponibilidad, zona local, zona Wavelength u Outpost.

Para iniciar la instancia en una zona de disponibilidad, seleccione la subred en la que desea iniciar la instancia. Para crear una subred, elija Crear nueva subred para ir a la consola de Amazon VPC. Cuando haya terminado, vuelva al asistente y elija el ícono Refresh (Actualizar) para cargar la subred en la lista.

Para iniciar la instancia en una zona local, seleccione una subred que haya creado en la zona local.

Para iniciar una instancia en un Outpost, seleccione una subred en una VPC que haya asociado a un Outpost.

- Firewall (grupos de seguridad): utilice uno o más grupos de seguridad para definir reglas de firewall para la instancia. Estas reglas especifican qué tráfico procedente de la red se entregará en la instancia. El resto del tráfico se ignora. Para obtener más información acerca de los grupos de seguridad, consulte Grupos de seguridad de Amazon EC2 para instancias EC2.

  Si agrega una interfaz de red, debe especificar los mismos grupos de seguridad en la interaz de red.

  Seleccione o cree un grupo de seguridad como se indica a continuación:

  - Para seleccionar un grupo de seguridad existente, hágalo desde la opción Select existing security group (Seleccionar un grupo de seguridad existente) y seleccione el grupo de seguridad de Common security groups (Grupos de seguridad comunes).
  - Para crear un grupo de seguridad, elija Create security group (Crear un grupo de seguridad).

    Puede añadir reglas para adaptarse a sus necesidades. Por ejemplo, si la instancia será un servidor web, abra los puertos 80 (HTTP) y 443 (HTTPS) para permitir el tráfico de Internet.

    Para agregar una regla, elija Add security group rule (Agregar regla de grupo de seguridad). En Type (Tipo), seleccione el tipo de tráfico de red. El campo Protocol (Protocolo) se rellena automáticamente con el protocolo para abrir al tráfico de red. En Source type (Tipo de origen) elija un tipo de origen. Para permitir que la plantilla de inicialización agregue la dirección IP pública de la computadora, elija My IP (Mi IP). Sin embargo, si se conecta a través de un ISP o protegido por su firewall sin una dirección IP estática, deberá encontrar el rango de direcciones IP utilizadas por los equipos cliente.

> **Warning**
>
> Las reglas que habilitan a todas las direcciones IP (`0.0.0.0/0`) para que puedan acceder a su instancia por SSH o RDP son aceptables si está por iniciar una instancia de prueba por un breve periodo y la detendrá o finalizará pronto, pero no es seguro para entornos de producción. Debe autorizar el acceso a su instancia únicamente a una dirección IP o a un rango de direcciones IP específico.

- Configuración de red avanzada

  Interfaz de red

  - Device index (Índice de dispositivo): el número de dispositivo para la interfaz de red, por ejemplo, `eth0` para la interfaz de red principal. Si deja el campo en blanco, AWS crea la interfaz de red principal.
  - Interfaz de red: seleccione Nueva interfaz para permitir que Amazon EC2 cree una interfaz nueva o seleccione una interfaz de red existente disponible.
  - Descripción: (Opcional) una descripción para la nueva interfaz de red.
  - Subnet (Subred): la subred en la que se creará una nueva interfaz de red. Para la interfaz de red principal (`eth0`), esta es la subred en la que se inicia la instancia. Si ha especificado una interfaz de red para `eth0`, se inicia la instancia en la subred en la que se encuentra la interfaz de red.
  - Grupos de seguridad: uno o más grupos de seguridad de la VPC a los que asociar la interfaz de red.
  - Auto-assign Public IP (Asignar IP pública automáticamente): especifique si la instancia recibe una dirección IPv4 pública. De forma predeterminada, las instancias en una subred predeterminada reciben una dirección IPv4 pública, mientras que las instancias en una subred no predeterminada no la reciben. Puede seleccionar Enable (Habilitar) o Disable (Deshabilitar) para anular la configuración predeterminada de la subred. Para obtener más información, consulte Direcciones IPv4 públicas.
  - IP principal: una dirección IPv4 privada del intervalo de su subred. Deje en blanco para permitir que Amazon EC2 elija una dirección IPv4 privada.
  - Secondary IP (IP secundaria): una o más direcciones IPv4 privadas del intervalo de la subred. Elija Manually assign (Asignar manualmente) e ingrese una dirección IP. Elija Add IP (Agregar IP) para agregar otra dirección IP. O bien, elija Asignar automáticamente para permitir que Amazon EC2 elija uno por usted e ingrese un valor para indicar el número de direcciones IP que desea agregar.

- (Solo IPv6) IPv6 IPs (IP IPv6): una dirección IPv6 del intervalo de la subred. Elija Manually assign (Asignar manualmente) e ingrese una dirección IP. Elija Add IP (Agregar IP) para agregar otra dirección IP. O bien, elija Asignar automáticamente para permitir que Amazon EC2 elija uno por usted e ingrese un valor para indicar el número de direcciones IP que desea agregar.
- Prefijos IPv4: los prefijos IPv4 para la interfaz de red.
- Prefijos IPv6: los prefijos IPv6 para la interfaz de red.
- (Opcional) Asignar IP IPv6 principal: si va a iniciar una instancia en una subred de doble pila o solo para IPv6, tiene la opción de Asignar IP IPv6 principal. La asignación de una dirección IPv6 principal le permite evitar interrumpir el tráfico a las instancias o ENI. Elija Habilitar si esta instancia depende de que su dirección IPv6 no cambie. Al iniciar la instancia, AWS asignará automáticamente una dirección IPv6 asociada al ENI adjunto a la instancia como la dirección IPv6 principal. Una vez que habilite una dirección GUA de IPv6 para que sea la IPv6 principal, no podrá deshabilitarla. Al habilitar una dirección GUA de IPv6 para que sea una de IPv6 principal, la primera dirección GUA de IPv6 pasará a ser la dirección IPv6 principal hasta que se termine la instancia o se separe la interfaz de red. Si tiene varias direcciones IPv6 asociadas a un ENI adjunto a su instancia y habilita una dirección IPv6 principal, la primera dirección GUA de IPv6 asociada al ENI pasa a ser la dirección IPv6 principal.
- Eliminar al terminar: si la interfaz de red se elimina, cuándo se elimina la instancia.
- Elastic Fabric Adapter: indica si la interfaz de red es un Elastic Fabric Adapter. Para obtener más información, consulte the section called “Elastic Fabric Adapter”.
- Índice de la tarjeta de red: el índice de la tarjeta de red. La interfaz de red principal debe asignarse al índice 0 de la tarjeta de red. Algunos tipos de instancia admiten varias tarjetas de red.
- ENA Express: ENA Express funciona con la tecnología de Scalable Reliable Datagram (SRD) de AWS. La tecnología SRD utiliza un mecanismo de difusión de paquetes para distribuir la carga y evitar la congestión de la red. Al habilitar ENA Express, las instancias compatibles se comunican mediante SRD además del tráfico de TCP normal siempre que sea posible. La plantilla de inicialización no incluye la configuración de ENA Express para la instancia, a menos que seleccione Habilitar o Deshabilitar.
- UDP de ENA Express: si habilitó ENA Express, de forma opcional, puede usar dicha característica para el tráfico de UDP. La plantilla de inicialización no incluye la configuración de ENA Express para la instancia, a menos que seleccione Habilitar o Deshabilitar.

Elija Add network interface (Agregar interfaz de red) para agregar más interfaces de la red. El número de interfaces de red que puede agregar depende del número admitido por el tipo de

instancia seleccionado. Las interfaces de red adicionales pueden residir en una subred distinta de la misma VPC o en una subred de una VPC diferente que posea (siempre que la subred se encuentre en la misma zona de disponibilidad que la instancia). Si selecciona una subred en otra VPC, la etiqueta de varias VPC se muestra junto a la interfaz de red que ha añadido. Esto le permite crear instancias con varios hosts en las VPC con diferentes configuraciones de red y seguridad. Tenga en cuenta que si adjunta una ENI adicional desde otra VPC, debe elegir un grupo de seguridad para la ENI desde esa VPC.

Para obtener más información, consulte Interfaces de red elásticas. Si especifica más de una interfaz de red, la instancia no puede recibir una dirección IPv4 pública. Además, si especifica una interfaz de red existente para eth0, no puede anular la configuración de la IPv4 pública de la subred con Auto-assign Public IP (Asignar IP pública automáticamente). Para obtener más información, consulte Asignar una dirección IPv4 pública durante la inicialización de la instancia.

Configurar almacenamiento

Si especifica una AMI para la plantilla de inicialización, la AMI incluye uno o más volúmenes de almacenamiento, incluido el volumen raíz (Volumen 1 (raíz AMI)). Se pueden especificar volúmenes adicionales para adjuntar a la instancia.

Se puede utilizar la vista Simple o Advanced (Avanzada). Con la vista Simple, se especifica el tamaño y el tipo de volumen. Para especificar todos los parámetros de volumen, elija la vista Advanced (Avanzada) (en la parte superior derecha de la tarjeta).

Para agregar un nuevo volumen, elija Add new volume (Agregar nuevo volumen).

Mediante el uso de la vista Advanced (Avanzada), puede configurar cada volumen de la siguiente manera:

- Storage type (Tipo de almacenamiento): el tipo de volumen (EBS o efímero) que desea asociar a la instancia. El tipo de volumen del almacén de instancias (efímero) solo está disponible si selecciona un tipo de instancia que lo admita. Para obtener más información, consulte Almacén de instancias Amazon EC2 y Volúmenes de Amazon EBS.
- Device name (Nombre de dispositivo): selecciónelo de la lista de nombres de dispositivo disponibles para el volumen.
- Snapshot (Instantánea): seleccione la instantánea desde la que desea crear un volumen. También puede buscar instantáneas públicas y compartidas disponibles escribiendo texto en el campo Snapshot (Instantánea).

- Size (GiB) (Tamaño [GiB]): para volúmenes de EBS, puede especificar un tamaño de almacenamiento. Si ha seleccionado una AMI y una instancia aptas para el nivel gratuito, recuerde que para permanecer en dicho nivel debe mantenerse por debajo de los 30 GiB de almacenamiento total.
- Volume type (Tipo de volumen): elija un tipo de volumen para volúmenes de EBS. Para obtener más información, consulte Tipos de volúmenes de Amazon EBS en la Guía del usuario de Amazon EBS.
- IOPS: si ha seleccionado un tipo de volumen de SSD de IOPS aprovisionadas (`io1` y `io2`) y SSD de uso general (`gp3`), puede ingresar el número de operaciones de E/S por segundo (IOPS) que puede admitir el volumen. Es necesario para los volúmenes io1, io2 y gp3. No se admite para los volúmenes gp2, st1, sc1 o estándar. Si se omite este parámetro para la plantilla de inicialización, se debe especificar un valor para él cuando se lance una instancia desde la plantilla de inicialización.
- Delete on termination (Eliminar al terminar): para los volúmenes de Amazon EBS, elija Yes (Sí) si se eliminará el volumen cuando se termine la instancia asociada o elija No para mantener el volumen. Para obtener más información, consulte Conservación de los datos cuando se termina una instancia.
- Encrypted (Cifrado): si el tipo de instancia admite el cifrado EBS, puede elegir Yes (Sí) para habilitar el cifrado para el volumen. Si ha habilitado el cifrado de forma predeterminada en esta región, el cifrado se habilita automáticamente. Para obtener más información, consulte Cifrado de Amazon EBS en la Guía del usuario de Amazon EBS.
- KMS key (Clave KMS): si ha seleccionado Yes (Sí) para Encrypted (Cifrado), a continuación, debe seleccionar una clave administrada por el cliente a fin de utilizarla para cifrar el volumen. Si ha habilitado el cifrado de forma predeterminada en esta región, se selecciona automáticamente la clave predeterminada administrada por el cliente. Puede seleccionar una clave diferente o especificar el ARN de cualquier clave administrada por el cliente que haya creado.

Etiquetas de recursos

Para etiquetar los recursos que se crean cuando se inicia una instancia, en Resource tags (Etiquetas de recursos), elija Add tag (Agregar etiqueta) y, a continuación, introduzca una clave de etiqueta y un par de valor. En Resource types (Tipos de recursos), especifique los recursos que se van a etiquetar durante la creación. Puede especificar la misma etiqueta para todos los recursos o especificar etiquetas diferentes para distintos recursos. Elija Add tag (Agregar etiqueta) para cada etiqueta adicional.

Puede especificar etiquetas para los siguientes recursos que se crean cuando se utiliza una plantilla de inicialización:

- instancias
- Volúmenes
- Solicitudes de instancia de spot
- Interfaces de red

> **Note**
>
> Para etiquetar la plantilla de inicio en sí, debe especificar las etiquetas en Template tags (Etiquetas de plantilla). Para obtener más información, consulte Nombre, descripción y etiquetas de la plantilla de inicialización.

Detalles avanzados

En Detalles avanzados, expanda la sección para ver los campos y especifique cualquier parámetro adicional para la instancia.

- Purchasing option (Opción de compra): elija Request Spot Instances (Solicitar instancias de spot) para solicitar instancias de spot al precio de spot, limitado al precio bajo demanda, y elija Customize (Personalizar) para cambiar la configuración de instancia de spot predeterminada. Puede establecer el precio máximo (no recomendado) y cambiar el tipo de solicitud, la duración de la solicitud y el comportamiento de interrupción. Si no solicita una instancia de spot, EC2 inicia una instancia bajo demanda de forma predeterminada. Para obtener más información, consulte Spot Instances.
- IAM instance profile (Perfil de instancias de IAM): seleccione un perfil de instancias de AWS Identity and Access Management (IAM) para asociarlo a la instancia. Para obtener más información, consulte Roles de IAM para Amazon EC2.
- Hostname type (Tipo de nombre de anfitrión): selecciónelo si desea que el nombre de host del sistema operativo invitado de la instancia incluya el nombre del recurso o el nombre de IP. Para obtener más información, consulte Tipos de nombres de host de instancias de Amazon EC2.
- DNS Hostname (Nombre de host DNS): determina si las consultas de DNS al nombre del recurso o de IP (según lo que haya seleccionado para Hostname type) responderán con la dirección IPv4

(registro A), dirección IPv6 (registro AAAA) o ambas. Para obtener más información, consulte Tipos de nombres de host de instancias de Amazon EC2.

- Shutdown behavior (Comportamiento de cierre): seleccione si la instancia debe detenerse o terminarse al cerrarla. Para obtener más información, consulte Cambiar el comportamiento de apagado iniciado por la instancia.
- Stop - Hibernate behavior (Detener: comportamiento de hibernación): para habilitar la hibernación, seleccione Enable (Habilitar). Este campo solo es válido para instancias que cumplen con los requisitos previos de hibernación. Para obtener más información, consulte Hibernación de la instancia de Amazon EC2.
- Termination protection (Protección de terminación): para evitar una terminación accidental, elija Enable (Habilitar). Para obtener más información, consulte Cómo habilitar la protección contra la terminación.
- Protección de detención: para evitar detenciones accidentales, elija Enable (Habilitar). Para obtener más información, consulte Habilitación de la protección de detención.
- Detailed CloudWatch monitoring (Monitoreo detallado de CloudWatch): elija Enable (Habilitar) si se debe activar el monitoreo detallado de la instancia con Amazon CloudWatch. Se aplican cargos adicionales. Para obtener más información, consulte Monitorear las instancias con CloudWatch.
- GPU elástica: Amazon Elastic Graphics llegó al final de su vida útil el 8 de enero de 2024. Para las cargas de trabajo que requieren aceleración de gráficos, le recomendamos usar instancias G4ad, G4dn o G5 de Amazon EC2.
- Inferencia elástica: acelerador de Elastic Inference a asociar a su instancia CPU EC2. Para obtener más información, consulte la sección sobre cómo trabajar con Amazon Elastic Inference en la guía para desarrolladores de Amazon Elastic Inference.

> **Note**
>
> A partir del 15 de abril de 2023, AWS no incorporará nuevos clientes a Amazon Elastic Inference (EI) y ayudará a los clientes actuales a migrar sus cargas de trabajo a opciones que ofrezcan un mejor precio y rendimiento. A partir del 15 de abril de 2023, los nuevos clientes no podrán iniciar instancias con los aceleradores de Amazon EI en Amazon SageMaker, Amazon ECS o Amazon EC2. Sin embargo, los clientes que hayan utilizado Amazon EI al menos una vez durante los últimos 30 días se consideran clientes actuales y podrán seguir utilizando el servicio.

- Credit specification (Especificación de crédito): elija Unlimited (Ilimitado) para permitir que las aplicaciones se expandan más allá de la base de referencia por el tiempo que sea necesario. Este

campo solo es válido para instancias T. Podrían aplicarse cargos adicionales. Para obtener más información, consulte Instancias de rendimiento ampliable.

- Nombre del grupo de ubicación: especifique el grupo de ubicación en el que desea iniciar la instancia. Se puede seleccionar un grupo de ubicación existente o crear uno nuevo. No todos los tipos de instancias se pueden iniciar en grupos de ubicación. Para obtener más información, consulte Grupos de ubicación.
- EBS-optimized instance (instancia optimizada para EBS): seleccione Enable (Habilitar) para proporciona capacidad dedicada adicional para la E/S de Amazon EBS. No todos los tipos de instancias admiten esta característica. Se aplican cargos adicionales. Para obtener más información, consulte the section called “Optimización de EBS”.
- Capacity Reservation (Reserva de capacidad): especifique si desea iniciar la instancia en cualquier reserva de capacidad abierta (Open [Abierta]), una reserva de capacidad específica (Target by ID [Destino por ID]) o un grupo de reserva de capacidad (Target by group [Destino por grupo]). Para especificar que no se debe utilizar una reserva de capacidad, elija None (Ninguna). Para obtener más información, consulte iniciar instancias en una Reserva de capacidad existente.
- Tenancy (Tenencia): elija si ejecutar su instancia en hardware compartido (Shared [Compartido]), asilado, hardware dedicado (Dedicated [Dedicado]) o en un host dedicado (Dedicated host [Host dedicado]). Si decide iniciar la instancia en host dedicado, puede especificar si desea iniciar la instancia en un grupo de recursos de host o utilizar un host dedicado específico como destino. Podrían aplicarse cargos adicionales. Para obtener más información, consulte Dedicated Instances y Dedicated Hosts.
- RAM disk ID (ID de disco RAM): (solo válido para AMI paravirtuales [PV]) seleccione un disco RAM para la instancia. Si ha seleccionado un kernel, puede que tenga que seleccionar un disco RAM específico con los controladores necesarios.
- Kernel ID (ID del kernel): (solo válido para AMI paravirtuales [PV]) seleccione un kernel para la instancia.
- Nitro Enclave: permite crear entornos de ejecución aislados, llamados enclaves, a partir de instancias de Amazon EC2. Seleccione Enable (Habilitar) para habilitar la instancia de Nitro Enclaves de AWS. Para obtener más información, consulte ¿Qué son los Nitro Enclaves de AWS? en la Guía del usuario de Nitro Enclaves de AWS.
- Configuraciones de licencia: puede iniciar instancias con la configuración de licencia especificada para realizar un seguimiento del uso de la licencia. Para obtener más información, consulte la sección Crear configuraciones de licencia en la Guía del usuario de License Manager de AWS.
- Specify CPU options (Especifique opciones de CPU): elija Specify CPU options (Especificar opciones de CPU) para especificar un número personalizado de CPU virtuales durante la

inicialización. Establezca el número de núcleos de la CPU y subprocesos por núcleo. Para obtener más información, consulte Optimización de las opciones de CPU.

- Punto de conexión IPv6 para la obtención de metadatos: puede permitir que una instancia utilice la dirección IPv6 del IMDS `[fd00:ec2::254]` para recuperar los metadatos de la instancia. Esta opción solo está disponible para el lanzamiento de instancias basadas en AWS Nitro System en una subred compatible con IPv6 (de doble pila o solo IPv6). Para obtener más información, consulte Recuperar metadatos de instancia.
- Metadatos accesibles: puede habilitar o deshabilitar el acceso a IMDS. Para obtener más información, consulte Configurar las opciones de metadatos para instancias nuevas.
- Versión de metadatos: si habilita el acceso a IMDS, puede optar por requerir el uso de la versión 2 del servicio de metadatos de instancia, al solicitar metadatos de instancia. Para obtener más información, consulte Configurar las opciones de metadatos para instancias nuevas.
- Límite de saltos de respuesta de metadatos: si habilita IMDS, puede establecer el número permitido de saltos de red para el token de metadatos. Para obtener más información, consulte Configurar las opciones de metadatos para instancias nuevas.
- Allow tags in metadata (Permitir etiquetas en metadatos): si selecciona Enable (Habilitar), la instancia permitirá acceder a todas las etiquetas de su instancia desde sus metadatos. Si no incluye esta configuración en la plantilla, de forma predeterminada, no se permitirá el acceso a las etiquetas en los metadatos de instancia. Para obtener más información, consulte Permitir acceso a etiquetas en metadatos de instancia.
- User data (Datos de usuario): puede especificar los datos de usuario para configurar una instancia durante la inicialización o para ejecutar un script de configuración. Para obtener más información, consulte Ejecución de comandos en la instancia de Amazon EC2 durante la inicialización.

AWS CLIEjemplo de

El siguiente ejemplo utiliza el comando create-launch-template para crear una plantilla de inicialización con el nombre y la configuración de instancias especificados.

```
aws ec2 create-launch-template \
    --launch-template-name TemplateForWebServer \
    --version-description WebVersion1 \
    --tag-specifications 'ResourceType=launch-
template,Tags=[{Key=purpose,Value=production}]' \
    --launch-template-data file://template-data.json
```

A continuación se muestra un ejemplo JSON que especifica los datos de la plantilla de inicialización para la configuración de la instancia. Guarde el JSON en un archivo e inclúyalo en el parámetro `--launch-template-data`, tal y como se muestra en el comando de ejemplo.

```
{
    "NetworkInterfaces": [{
        "AssociatePublicIpAddress": true,
        "DeviceIndex": 0,
        "Ipv6AddressCount": 1,
        "SubnetId": "subnet-7b16de0c"
    }],
    "ImageId": "ami-8c1be5f6",
    "InstanceType": "r4.4xlarge",
    "TagSpecifications": [{
        "ResourceType": "instance",
        "Tags": [{
            "Key":"Name",
            "Value":"webserver"
        }]
    }],
    "CpuOptions": {
        "CoreCount":4,
        "ThreadsPerCore":2
    }
}
```

A continuación, se muestra un ejemplo del resultado.

```
{
    "LaunchTemplate": {
        "LatestVersionNumber": 1,
        "LaunchTemplateId": "lt-01238c059e3466abc",
        "LaunchTemplateName": "TemplateForWebServer",
        "DefaultVersionNumber": 1,
        "CreatedBy": "arn:aws:iam::123456789012:root",
        "CreateTime": "2017-11-27T09:13:24.000Z"
    }
}
```

AWS Tools for Windows PowerShellEjemplo de

En el siguiente ejemplo, se usa el cmdlet New-EC2LaunchTemplate para crear una plantilla de inicialización con el nombre y la configuración de instancias especificados.

```
$launchTemplateData = [Amazon.EC2.Model.RequestLaunchTemplateData]@{
    ImageId = 'ami-8c1be5f6'
    InstanceType = 'r4.4xlarge'
    NetworkInterfaces = @(
        [Amazon.EC2.Model.LaunchTemplateInstanceNetworkInterfaceSpecificationRequest]@{
            AssociatePublicIpAddress = $true
            DeviceIndex = 0
            Ipv6AddressCount = 1
            SubnetId = 'subnet-7b16de0c'
        }
    )
    TagSpecifications = @(
        [Amazon.EC2.Model.LaunchTemplateTagSpecificationRequest]@{
            ResourceType = 'instance'
            Tags = [Amazon.EC2.Model.Tag]@{
                Key = 'Name'
                Value = 'webserver'
            }
        }
    )
    CpuOptions = [Amazon.EC2.Model.LaunchTemplateCpuOptionsRequest]@{
        CoreCount = 4
        ThreadsPerCore = 2
    }
}
$tagSpecificationData = [Amazon.EC2.Model.TagSpecification]@{
    ResourceType = 'launch-template'
    Tags = [Amazon.EC2.Model.Tag]@{
        Key = 'purpose'
        Value = 'production'
    }
}
New-EC2LaunchTemplate -LaunchTemplateName 'TemplateForWebServer' -VersionDescription
 'WebVersion1' -LaunchTemplateData $launchTemplateData -TagSpecification
 $tagSpecificationData
```

A continuación, se muestra un ejemplo del resultado.

```
CreatedBy            : arn:aws:iam::123456789012:root
CreateTime           : 9/19/2023 16:57:55
DefaultVersionNumber : 1
LatestVersionNumber  : 1
LaunchTemplateId     : lt-01238c059eEXAMPLE
LaunchTemplateName   : TemplateForWebServer
Tags                 : {purpose}
```

Crear una plantilla de inicialización a partir de una existente

Puede clonar una plantilla de inicialización existente y luego ajustar los parámetros para crear una nueva plantilla de inicialización. Sin embargo, solo puede hacerlo cuando utiliza la consola de Amazon EC2; la AWS CLI no admite la clonación de una plantilla.

Console

Para crear una plantilla de inicialización a partir de una existente

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Launch Templates (Plantillas de inicialización) y, a continuación, Create launch template (Crear plantilla de inicialización).
3. En Nombre de plantilla de inicialización, introduzca un nombre descriptivo para la plantilla.
4. En Template version description (Descripción de la versión de plantilla), ingrese una breve descripción para esta versión de la plantilla de inicialización.
5. Para etiquetar la plantilla de inicialización durante la creación, expanda Template tags (Etiquetas de la plantilla), elija Add Tag (Agregar etiqueta) y, a continuación, introduzca un par de clave y un valor de etiqueta.
6. Expanda Plantilla de origen y para Nombre de la plantilla de inicialización, elija una plantilla de inicialización en la que basar la nueva plantilla de inicialización.
7. En Source template version (Versión de la plantilla de origen), elija la versión de la plantilla de inicialización en la que desea basar la plantilla nueva.
8. Ajuste los parámetros de inicialización según sea necesario y elija Create launch template (Crear plantilla de inicialización).

Crear una plantilla de inicialización a partir de una instancia

Console

Para crear una plantilla de inicialización a partir de una instancia

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Seleccione la instancia y elija Actions (Acciones), Create Template from Instance (Crear plantilla desde instancia).
4. Proporcione un nombre, descripción, etiquetas y ajuste los parámetros de inicialización según sea necesario.

> **Note**
>
> Cuando cree una plantilla de inicialización desde una instancia, las direcciones IP y los ID de la interfaz de red de la instancia no estarán incluidos en la plantilla.

5. Elija Create launch template (Crear plantilla de inicialización).

AWS CLI

Puede utilizar la AWS CLI para crear una plantilla de inicialización a partir de una instancia existente obteniendo primero los datos de la plantilla de inicialización de una instancia y, a continuación, creando una plantilla de inicialización con los datos de la plantilla de inicialización.

Para obtener los datos de la plantilla de inicialización a partir de una instancia

- Utilice el comando get-launch-template-data y especifique el ID de la instancia. Puede usar la salida como base para crear una nueva plantilla de inicialización o una versión. De forma predeterminada, la salida incluye un objeto de nivel superior `LaunchTemplateData`, que no puede especificarse en los datos de su plantilla de inicialización. Utilice la opción `--query` para excluir este objeto.

```
aws ec2 get-launch-template-data \
    --instance-id i-0123d646e8048babc \
    --query "LaunchTemplateData"
```

A continuación, se muestra un ejemplo del resultado.

```
{
    "Monitoring": {},
    "ImageId": "ami-8c1be5f6",
    "BlockDeviceMappings": [
        {
            "DeviceName": "/dev/xvda",
            "Ebs": {
                "DeleteOnTermination": true
            }
        }
    ],
    "EbsOptimized": false,
    "Placement": {
        "Tenancy": "default",
        "GroupName": "",
        "AvailabilityZone": "us-east-1a"
    },
    "InstanceType": "t2.micro",
    "NetworkInterfaces": [
        {
            "Description": "",
            "NetworkInterfaceId": "eni-35306abc",
            "PrivateIpAddresses": [
                {
                    "Primary": true,
                    "PrivateIpAddress": "10.0.0.72"
                }
            ],
            "SubnetId": "subnet-7b16de0c",
            "Groups": [
                "sg-7c227019"
            ],
            "Ipv6Addresses": [
                {
                    "Ipv6Address": "2001:db8:1234:1a00::123"
                }
            ],
            "PrivateIpAddress": "10.0.0.72"
        }
    ]
```

```
    }
```

Puede escribir la salida directamente en un archivo; por ejemplo:

```
aws ec2 get-launch-template-data \
    --instance-id i-0123d646e8048babc \
    --query "LaunchTemplateData" >> instance-data.json
```

Para crear una plantilla de inicialización con datos de plantilla de inicialización

- Utilice el comando create-launch-template para crear una plantilla de inicialización utilizando el resultado del procedimiento anterior. Para obtener más información acerca de cómo crear una plantilla de inicialización mediante la AWS CLI, consulte Creación de una plantilla de inicialización a partir de parámetros.

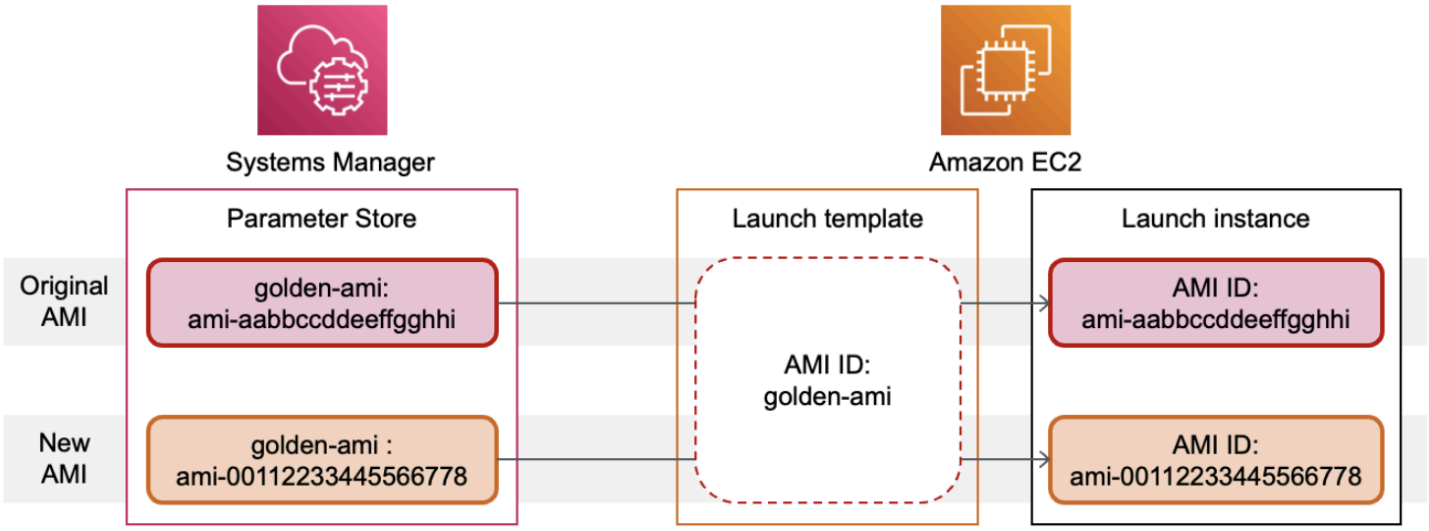
Uso de un parámetro de Systems Manager en lugar de un ID de AMI

En lugar de especificar un ID de AMI en las plantillas de inicialización, puede especificar un parámetro AWS Systems Manager. Si el ID de AMI cambia, puede actualizar el ID de AMI en un lugar actualizando el parámetro de Systems Manager en el almacén de parámetros de Systems Manager. Los parámetros también se pueden compartir con otras Cuentas de AWS. Puede almacenar y administrar de forma centralizada los parámetros de la AMI en una cuenta y compartirlos con todas las otras que necesiten hacer referencia a ellos. Mediante el uso de un parámetro de Systems Manager, todas las plantillas de inicialización se pueden actualizar en una sola acción.

Un parámetro de Systems Manager es un par clave-valor definido por el usuario que crea en el almacén de parámetros de Systems Manager. El almacén de parámetros proporciona una base central para almacenar los valores de configuración de la aplicación. Para obtener más información, consulte Almacén de parámetros de AWS Systems Manager en la Guía del usuario de AWS Systems Manager.

En el siguiente diagrama, el parámetro `golden-ami` se asigna primero a la AMI original `ami-aabbccddeeffgghhi` en el almacén de parámetros. En la plantilla de inicialización, el valor del ID de AMI es `golden-ami`. Cuando se inicia una instancia con esta plantilla de inicialización, el ID de AMI se transforma en `ami-aabbccddeeffgghhi`. Posteriormente, la AMI se actualiza, lo que da como resultado un nuevo ID de AMI. En el almacén de parámetros, el parámetro `golden-ami` se asigna al nuevo `ami-00112233445566778`. La plantilla de inicialización permanece sin cambios.

Cuando se inicia una instancia con esta plantilla de inicialización, el ID de AMI se convierte en el nuevo `ami-00112233445566778`.



Formato de parámetros de Systems Manager para identificadores de AMI

Las plantillas de inicialización requieren que los parámetros de Systems Manager definidos por el usuario sigan el siguiente formato cuando se usen en lugar de un ID de AMI:

- Tipo de parámetro: `String`
- Tipo de datos de parámetros: `aws:ec2:image`: esto garantiza que el almacén de parámetros valide que el valor ingresado tenga el formato adecuado para un ID de AMI.

Para obtener más información sobre cómo crear un parámetro válido para un ID de AMI, consulte Creación de parámetros de Systems Manager en la Guía del usuario de AWS Systems Manager.

Formato de parámetros de Systems Manager en plantillas de inicialización

Para utilizar un parámetro de Systems Manager en lugar de un ID de AMI en una plantilla de inicialización, debe utilizar uno de los siguientes formatos al especificar el parámetro en la plantilla de inicialización:

Para hacer referencia a un parámetro público:

- `resolve:ssm:`*`public-parameter`*

Para hacer referencia a un parámetro almacenado en la misma cuenta:

- `resolve:ssm:parameter-name`
- `resolve:ssm:parameter-name:version-number`: el número de versión en sí mismo es una etiqueta por defecto
- `resolve:ssm:parameter-name:label`

Para hacer referencia a un parámetro compartido desde otra Cuenta de AWS:

- `resolve:ssm:parameter-ARN`
- `resolve:ssm:parameter-ARN:version-number`
- `resolve:ssm:parameter-ARN:label`

Versiones de parámetros

Los parámetros de Systems Manager son recursos versionados. Al actualizar un parámetro, se crean versiones nuevas y sucesivas del parámetro. Systems Manager admite etiquetas de parámetros que se pueden asignar a versiones específicas de un parámetro.

Por ejemplo, el parámetro `golden-ami` puede tener tres versiones: `1`, `2`, y `3`. Puede crear una etiqueta de parámetro `beta` que se asigne a la versión `2` y una etiqueta de parámetro `prod` que se asigne a la versión`3`.

En una plantilla de inicialización, puede especificar la versión 3 del parámetro `golden-ami` mediante uno de los siguientes formatos:

- `resolve:ssm:golden-ami:3`
- `resolve:ssm:golden-ami:prod`

La especificación de la versión o la etiqueta es opcional. Cuando no se especifica ninguna versión ni etiqueta, se utiliza la última versión del parámetro.

Especificación de un parámetro de Systems Manager en una plantilla de inicialización

Puede especificar un parámetro de Systems Manager en una plantilla de inicialización en lugar de un ID de AMI al crear una plantilla de inicialización o una nueva versión de una plantilla de inicialización.

Console

Especificación de un parámetro de Systems Manager en una plantilla de inicialización

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Launch Templates (Plantillas de inicialización) y, a continuación, Create launch template (Crear plantilla de inicialización).
3. En Launch template name (Nombre de plantilla de inicialización), introduzca un nombre descriptivo para la plantilla.
4. En Application and OS Images (Imagen de máquina de Amazon) (Imágenes de aplicaciones y sistema operativo [imagen de máquina de Amazon]), elija Browse more AMIs (Buscar más AMI).
5. Elija el botón de flecha situado a la derecha de la barra de búsqueda y luego elija Especificar valor personalizado/parámetro de Systems Manager.
6. En el cuadro de diálogo Especificar valor personalizado o parámetro de Systems Manager, haga lo siguiente:

   a. Para el ID de AMI o la cadena de parámetros de Systems Manager, introduzca el nombre del parámetro de Systems Manager mediante uno de los siguientes formatos:

      Para hacer referencia a un parámetro público:

      - **resolve:ssm:*public-parameter***

      Para hacer referencia a un parámetro almacenado en la misma cuenta:

      - **resolve:ssm:*parameter-name***
      - **resolve:ssm:*parameter-name*:*version-number***
      - **resolve:ssm:*parameter-name*:*label***

      Para hacer referencia a un parámetro compartido desde otra Cuenta de AWS:

      - **resolve:ssm:*parameter-ARN***
      - **resolve:ssm:*parameter-ARN*:*version-number***
      - **resolve:ssm:*parameter-ARN*:*label***

   b. Seleccione Guardar.

7. Especifique cualquier otro parámetro de la plantilla de inicialización según sea necesario y, a continuación, seleccione Crear plantilla de inicialización.

Para obtener más información, consulte Creación de una plantilla de inicialización a partir de parámetros.

AWS CLI

Especificación de un parámetro de Systems Manager en una plantilla de inicialización

- Utilice el comando create-launch-template (crear una plantilla de inicialización) para crear la plantilla de inicialización. Para especificar la AMI que se va a utilizar, introduzca el nombre del parámetro de Systems Manager con uno de los siguientes formatos:

  Para hacer referencia a un parámetro público:

  - **resolve:ssm:*public-parameter***

  Para hacer referencia a un parámetro almacenado en la misma cuenta:

  - **resolve:ssm:*parameter-name***
  - **resolve:ssm:*parameter-name*:*version-number***
  - **resolve:ssm:*parameter-name*:*label***

  Para hacer referencia a un parámetro compartido desde otra Cuenta de AWS:

  - **resolve:ssm:*parameter-ARN***
  - **resolve:ssm:*parameter-ARN*:*version-number***
  - **resolve:ssm:*parameter-ARN*:*label***

  En el siguiente ejemplo se crea una plantilla de inicialización que especifica lo siguiente:

  - Un nombre para la plantilla de inicialización (*TemplateForWebServer*)
  - Una etiqueta para la plantilla de inicialización (*purpose*=*production*)
  - Los datos de la configuración de la instancia, especificados en un archivo JSON:
    - La AMI que se va a utilizar (`resolve:ssm:`*golden-ami*)
    - El tipo de instancia que va a iniciar (*m5.4xlarge*)

- Una etiqueta para la instancia (*Name*=*webserver*)

```
aws ec2 create-launch-template \
    --launch-template-name TemplateForWebServer \
    --tag-specifications 'ResourceType=launch-
template,Tags=[{Key=purpose,Value=production}]' \
    --launch-template-data file://template-data.json
```

A continuación se muestra un archivo JSON de ejemplo que contiene los datos de la plantilla de inicialización de la configuración de la instancia. El valor de `ImageId` es el nombre del parámetro de Systems Manager, introducido en el formato requerido `resolve:ssm:golden-ami`.

```
{"LaunchTemplateData": {
    "ImageId": "resolve:ssm:golden-ami",
    "InstanceType": "m5.4xlarge",
    "TagSpecifications": [{
        "ResourceType": "instance",
        "Tags": [{
            "Key":"Name",
            "Value":"webserver"
        }]
    }]
  }
}
```

Verificación de que la plantilla de inicialización tenga el ID de AMI correcto

Cómo convertir el parámetro de Systems Manager en el ID de AMI real

Utilice el comando describe-launch-template-versions e incluya el parámetro `--resolve-alias`.

```
aws ec2 describe-launch-template-versions \
    --launch-template-name my-launch-template \
    --versions $Default \
    --resolve-alias
```

La respuesta incluye el ID de AMI para el `ImageId`. En este ejemplo, cuando se inicializa una instancia utilizando esta plantilla de inicialización, el ID de AMI se resuelve como `ami-0ac394d6a3example`.

```
{
    "LaunchTemplateVersions": [
        {
            "LaunchTemplateId": "lt-089c023a30example",
            "LaunchTemplateName": "my-launch-template",
            "VersionNumber": 1,
            "CreateTime": "2022-12-28T19:52:27.000Z",
            "CreatedBy": "arn:aws:iam::123456789012:user/Bob",
            "DefaultVersion": true,
            "LaunchTemplateData": {
                "ImageId": "ami-0ac394d6a3example",
                "InstanceType": "t3.micro",
            }
        }
    ]
}
```

Recursos relacionados

Para obtener más información sobre cómo trabajar con parámetros de Systems Manager, consulte los siguientes materiales de referencia en la documentación de Systems Manager.

- Para obtener información sobre cómo buscar los parámetros públicos de la AMI compatibles con Amazon EC2, consulte Calling AMI public parameters.
- Para obtener información sobre cómo compartir parámetros con otras cuentas de AWS o a través de AWS Organizations, consulte Working with shared parameters.
- Para obtener información sobre la supervisión para controlar si los parámetros se crearon correctamente, consulte Native parameter support for Amazon Machine Image IDs.

Limitaciones

- Actualmente, las flotas de EC2 y las flotas de spot no admiten el uso de una plantilla de inicialización que tenga un parámetro de Systems Manager especificado en lugar de un ID de AMI. Para EC2 Fleets y Spot Fleets, si especifica una AMI en la plantilla de inicialización, debe especificar el ID de AMI.

- Amazon EC2 Auto Scaling ofrece otras restricciones. Para obtener más información, consulte Use AWS Systems Manager parameters instead of AMI IDs in launch templates en la Guía del usuario de Amazon EC2 Auto Scaling.

Modificar una plantilla de inicialización (administrar versiones de plantillas de inicialización)

Las plantillas de inicialización son inmutables; después de crear una plantilla de inicialización, no podrá modificarla. En cambio, puede crear una nueva versión de la plantilla de inicialización que incluya los cambios que necesite.

Puede crear diferentes versiones de una plantilla de inicialización, definir la versión predeterminada, describir una versión de plantilla de inicialización y eliminar las que ya no necesite.

Tareas

- Crear una versión de plantilla de inicialización
- Establecer la versión de la plantilla de inicialización predeterminada
- Describir una versión de una plantilla de inicialización
- Eliminar una versión de plantilla de inicialización

Crear una versión de plantilla de inicialización

Al crear una versión de una plantilla de inicialización, puede especificar parámetros nuevos o usar una versión que ya esté disponible como base para la nueva. Para obtener más información acerca de los parámetros de inicialización, consulte Creación de una plantilla de lanzamiento.

Console

Para crear una versión de plantilla de inicialización

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Launch Templates (Plantillas de inicialización).
3. Seleccione una plantilla de inicialización y, a continuación, elija Actions (Acciones), Modify template (Create new version) (Modificar plantilla (Crear nueva versión)).
4. En Template version description (Descripción de la versión de plantilla), escriba una descripción para esta versión de la plantilla de inicialización.
5. (Opcional) Expanda la Source template (Plantilla de origen) y seleccione una versión de la plantilla de inicialización para utilizarla como base para la nueva versión de la plantilla

de inicialización. La nueva versión de plantilla de inicialización hereda los parámetros de inicialización de esta versión de plantilla de inicialización.

6. Modifique los parámetros de inicialización según sea necesario y elija Create launch template (Crear plantilla de inicialización).

AWS CLI

Para crear una versión de plantilla de inicialización

- Utilice el comando create-launch-template-version. Puede especificar una versión de origen en la que basar la nueva. La nueva versión hereda los parámetros de inicialización de esta versión, pero puede invalidarlos con `--launch-template-data`. En el siguiente ejemplo, se crea una nueva versión basada en la versión 1 de la plantilla de inicialización y se especifica un ID de AMI diferente.

```
aws ec2 create-launch-template-version \
    --launch-template-id lt-0abcd290751193123 \
    --version-description WebVersion2 \
    --source-version 1 \
    --launch-template-data "ImageId=ami-c998b6b2"
```

Establecer la versión de la plantilla de inicialización predeterminada

Puede definir la versión predeterminada de una plantilla de inicialización. Si no especifica una versión al iniciar una instancia desde una plantilla de inicialización, se inicia con los parámetros de la versión predeterminada.

Console

Para establecer la versión de la plantilla de inicialización predeterminada

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Launch Templates (Plantillas de inicialización).
3. Seleccione la plantilla de inicialización que desee y elija Actions (Acciones), seguido de Set default version (Establecer versión predeterminada).

4. En Template version (Versión de plantilla), seleccione el número de versión que desea establecer como versión predeterminada y elija Set as default version (Establecer como versión predeterminada).

AWS CLI

Para establecer la versión de la plantilla de inicialización predeterminada

- Utilice el comando modify-launch-template y especifique la versión que desea definir como predeterminada.

```
aws ec2 modify-launch-template \
    --launch-template-id lt-0abcd290751193123 \
    --default-version 2
```

Describir una versión de una plantilla de inicialización

Con la consola, puede ver todas las versiones de la plantilla de inicialización seleccionada u obtener una lista de las plantillas de inicialización cuya versión más reciente o predeterminada coincida con un número de versión específico. Con la AWS CLI, puede describir todas las versiones, versiones individuales o un rango de versiones de una plantilla de inicialización especificada. También puede describir todas las versiones más recientes o todas las versiones predeterminadas de todas las plantillas de inicialización de su cuenta.

Console

Para describir una versión de una plantilla de inicialización

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Launch Templates (Plantillas de inicialización).
3. Puede ver una versión de una plantilla de inicialización específica u obtener una lista de las plantillas de inicialización cuya versión más reciente o predeterminada coincida con un número de versión específico.
   - Para ver la versión de una plantilla de inicialización: seleccione la plantilla de inicialización. En la pestaña Versiones, en Versión, seleccione una versión para ver sus detalles.

- Para obtener una lista de todas las plantillas de inicialización cuya última versión coincida con un número de versión específico: en la barra de búsqueda, elija Última versión, y, a continuación, seleccione un número de versión.
- Para obtener una lista de todas las plantillas de inicialización cuya última versión predeterminada coincida con un número de versión específico: en la barra de búsqueda, elija Versión predeterminada, y, a continuación, seleccione un número de versión.

AWS CLI

Para describir una versión de una plantilla de inicialización

- Utilice el comando describe-launch-template-versions y especifique los números de versión. En el siguiente ejemplo, se especifican las versiones *1* y *3*.

```
aws ec2 describe-launch-template-versions \
    --launch-template-id lt-0abcd290751193123 \
    --versions 1 3
```

Para describir todas las versiones de la plantilla de inicialización más recientes y predeterminadas de la cuenta

- Utilice el comando describe-launch-template-versions y especifique `$Latest`, `$Default` o ambos. Debe omitir el ID de la plantilla de inicialización y el nombre en la llamada. No se pueden especificar números de versión.

```
aws ec2 describe-launch-template-versions \
    --versions "$Latest,$Default"
```

Eliminar una versión de plantilla de inicialización

Si ya no necesita una versión de plantillla de inicialización en concreto, puede eliminarla.

Consideraciones

- No puede sustituir el número de versión después de eliminarlo.

- No puede eliminar la versión predeterminada de la plantilla de inicialización. Para poder hacerlo, primero debe asignar otra como predeterminada. Si la versión predeterminada es la única versión para la plantilla de inicialización, debe eliminar toda la plantilla de inicialización.
- Al utilizar la consola, puede eliminar una versión de la plantilla de inicialización a la vez. Cuando se utiliza la AWS CLI, puede eliminar hasta 200 versiones de plantillas de inicialización en una sola solicitud. Para eliminar más de 200 versiones en una sola solicitud, puede eliminar la plantilla de inicialización, que también elimina todas sus versiones.

Console

Para eliminar una versión de plantilla de inicialización

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Launch Templates (Plantillas de inicialización).
3. Seleccione la plantilla de inicialización que desee y elija Actions (Acciones), seguido de Delete template version (Eliminar versión de plantilla).
4. Seleccione la versión que desea eliminar y elija Delete (Eliminar).

AWS CLI

Para eliminar una versión de plantilla de inicialización

- Utilice el comando delete-launch-template-versions y especifique los números de versión que desea eliminar. Puede especificar hasta 200 versiones de plantillas de inicialización para eliminarlas en una sola solicitud.

```
aws ec2 delete-launch-template-versions \
    --launch-template-id lt-0abcd290751193123 \
    --versions 1
```

Eliminación de una plantilla de inicialización

Si ya no necesita una plantillla de inicialización en concreto, puede eliminarla. Al eliminar una plantilla de inicialización, también se eliminan todas sus versiones. Para eliminar una versión específica de una plantilla de inicialización, consulte Eliminar una versión de plantilla de inicialización.

Cuando elimina una plantilla de inicialización, esto no afecta a las instancias que haya iniciado desde la plantilla de inicialización.

Console

Para eliminar una plantilla de inicialización

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Launch Templates (Plantillas de inicialización).
3. Seleccione la plantilla de inicialización que desee y elija Actions (Acciones), seguido de Delete template (Eliminar plantilla).
4. Escriba **`Delete`** para confirmar la eliminación y, a continuación, elija Delete (Eliminar).

AWS CLI

Para eliminar una plantilla de inicialización

- Utilice el comando delete-launch-template (AWS CLI) y especifique la plantilla de inicialización.

```
aws ec2 delete-launch-template --launch-template-id lt-01238c059e3466abc
```

iniciar instancias desde una plantilla de inicialización

Las plantillas de inicialización son compatibles con varios servicios de inicialización de instancias. En este tema se describe cómo utilizar una plantilla de inicialización al iniciar una instancia con el asistente de inicialización de EC2, Amazon EC2 Auto Scaling, una flota de EC2 o una flota de spot.

Temas

- iniciar una instancia desde una plantilla de inicialización
- Usar plantillas de inicialización con Amazon EC2 Auto Scaling
- Usar plantillas de inicialización con flota de EC2
- Usar plantillas de inicialización con la flota de spot

iniciar una instancia desde una plantilla de inicialización

Puede usar los parámetros incluidos en una plantilla de inicialización para iniciar una instancia. También puede omitir o añadir parámetros de inicialización antes de iniciar la instancia.

A las instancias que se inician mediante una plantilla de inicialización se le asignan automáticamente dos etiquetas con las claves `aws:ec2launchtemplate:id` y `aws:ec2launchtemplate:version`. Estas etiquetas no se pueden eliminar ni editar.

Console

Para iniciar una instancia desde una plantilla de inicialización mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Launch Templates (Plantillas de inicialización).
3. Seleccione la plantilla de inicialización que desee y elija Actions (Acciones), seguido de Launch instance from template (iniciar instancia desde una plantilla).
4. En Source template version (Versión de la plantilla de origen), seleccione la versión de la plantilla de inicialización que desee utilizar.
5. En Number of instances (Número de instancias), especifique el número de instancias que desea iniciar.
6. (Opcional) Puede omitir o añadir parámetros de plantillas de inicialización cambiándolos o incluyéndolos en la sección Instance details (Detalles de la instancia).
7. Elija Launch instance from template (iniciar instancia desde una plantilla).

AWS CLI

inicialización de una instancia desde una plantilla de inicialización mediante la AWS CLI

- Utilice el comando run-instances y especifique el parámetro `--launch-template`. Opcionalmente, seleccione la versión de la plantilla de inicialización que usar. Si no especifica la versión, se usa la predeterminada.

```
aws ec2 run-instances \
    --launch-template LaunchTemplateId=lt-0abcd290751193123,Version=1
```

- Para omitir un parámetro de plantilla de inicialización, especifíquelo en el comando run-instances. En el siguiente ejemplo, se omite el tipo de instancia especificado en la plantilla de inicialización (de haberla).

```
aws ec2 run-instances \
    --launch-template LaunchTemplateId=lt-0abcd290751193123 \
    --instance-type t2.small
```

- Si especifica un parámetro anidado parte de una estructura compleja, la instancia se inicia mediante una estructura completa tal y como se especifica en la plantilla de inicialización, además de con cualquier otro parámetro anidado que especifique.

  En el siguiente ejemplo, la instancia se inicia con la etiqueta *Owner*=*TeamA*, entre otras especificadas en la plantilla de inicialización. Si la plantilla de inicialización ya incluye una etiqueta con una clave de *Owner*, el valor se sustituye por *TeamA*.

```
aws ec2 run-instances \
    --launch-template LaunchTemplateId=lt-0abcd290751193123 \
    --tag-specifications "ResourceType=instance,Tags=[{Key=Owner,Value=TeamA}]"
```

  En el siguiente ejemplo, la instancia se inicia con un volumen con el nombre de dispositivo */dev/xvdb*, entre otros mapeos de dispositivos de bloques especificados en la plantilla de inicialización. Si la plantilla de inicialización ya incluye un volumen definido en */dev/xvdb*, sus valores se sustituyen por los especificados.

```
aws ec2 run-instances \
    --launch-template LaunchTemplateId=lt-0abcd290751193123 \
    --block-device-mappings "DeviceName=/dev/
xvdb,Ebs={VolumeSize=20,VolumeType=gp2}"
```

Si se produce un error al iniciar la instancia o el estado pasa inmediatamente a `terminated` en lugar de `running`, consulte Solucionar problemas de lanzamiento de instancias.

PowerShell

inicialización de una instancia desde una plantilla de inicialización mediante la AWS Tools for PowerShell

- Use el comando Stop-EC2Instance y especifique el parámetro `-LaunchTemplate`. Opcionalmente, seleccione la versión de la plantilla de inicialización que usar. Si no especifica la versión, se usa la predeterminada.

```
Import-Module AWS.Tools.EC2
New-EC2Instance `
    -LaunchTemplate (
        New-Object -TypeName Amazon.EC2.Model.LaunchTemplateSpecification -
Property @{
            LaunchTemplateId = 'lt-0abcd290751193123';
            Version          = '4'
    }
)
```

- Para anular un parámetro de plantilla de inicialización, especifique el parámetro en el comando New-EC2Instance. En el siguiente ejemplo, se omite el tipo de instancia especificado en la plantilla de inicialización (de haberla).

```
Import-Module AWS.Tools.EC2
New-EC2Instance `
    -InstanceType t4g.small `
    -LaunchTemplate (
        New-Object -TypeName Amazon.EC2.Model.LaunchTemplateSpecification -
Property @{
            LaunchTemplateId = 'lt-0abcd290751193123';
            Version          = '4'
    }
)
```

- Si especifica un parámetro anidado parte de una estructura compleja, la instancia se inicia mediante una estructura completa tal y como se especifica en la plantilla de inicialización, además de con cualquier otro parámetro anidado que especifique.

  En el siguiente ejemplo, la instancia se inicia con la etiqueta *Owner*=*TeamA*, entre otras especificadas en la plantilla de inicialización. Si la plantilla de inicialización ya incluye una etiqueta con una clave de *Owner*, el valor se sustituye por *TeamA*.

```
Import-Module AWS.Tools.EC2
New-EC2Instance `
    -InstanceType t4g.small  `
    -LaunchTemplate (
        New-Object -TypeName Amazon.EC2.Model.LaunchTemplateSpecification -
Property @{
            LaunchTemplateId = 'lt-0abcd290751193123';
            Version          = '4'
        }
) `
    -TagSpecification (
        New-Object -TypeName Amazon.EC2.Model.TagSpecification -Property @{
            ResourceType = 'instance';
            Tags         = @(
                @{key = "Owner"; value = "TeamA" },
                @{key = "Department"; value = "Operations" }
            )
        }
)
```

En el siguiente ejemplo, la instancia se inicia con un volumen con el nombre de dispositivo */dev/xvdb*, entre otros mapeos de dispositivos de bloques especificados en la plantilla de inicialización. Si la plantilla de inicialización ya incluye un volumen definido en */dev/xvdb*, sus valores se sustituyen por los especificados.

```
Import-Module AWS.Tools.EC2
New-EC2Instance `
    -InstanceType t4g.small  `
    -LaunchTemplate (
        New-Object -TypeName Amazon.EC2.Model.LaunchTemplateSpecification -
Property @{
            LaunchTemplateId = 'lt-0abcd290751193123';
            Version          = '4'
    }
) `
    -BlockDeviceMapping  (
        New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping -Property @{
            DeviceName = '/dev/xvdb';
            EBS        = (
                New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice -Property @{
                    VolumeSize = 25;
```

```
                    VolumeType = 'gp3'
                }
            )
        }
)
```

Si se produce un error al iniciar la instancia o el estado pasa inmediatamente a `terminated` en lugar de `running`, consulte Solucionar problemas de lanzamiento de instancias.

Usar plantillas de inicialización con Amazon EC2 Auto Scaling

Puede crear un grupo de Auto Scaling y especificar una plantilla de inicialización para usarla con dicho grupo. Cuando Amazon EC2 Auto Scaling inicia instancias en el grupo de Auto Scaling, utiliza los parámetros de inicialización definidos en la plantilla de inicialización asociada. Para obtener más información, consulte Create a launch template for an Auto Scaling group y Create a launch template using advanced settings en la Guía del usuario de Amazon EC2 Auto Scaling.

Para poder crear un grupo de escalado automático con una plantilla de inicialización, debe crear una plantilla que incluya los parámetros necesarios para iniciar una instancia de EC2 en un grupo de escalado automático, como el ID de la AMI. La consola proporciona orientación para ayudarlo a crear una plantilla que pueda utilizar con Amazon EC2 Auto Scaling.

Para crear una plantilla de inicialización para utilizarla con Auto Scaling y la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Launch Templates (Plantillas de inicialización) y, a continuación, Create launch template (Crear plantilla de inicialización).
3. En Nombre de plantilla de inicialización, introduzca un nombre descriptivo para la plantilla.
4. En Template version description (Descripción de la versión de plantilla), ingrese una breve descripción para esta versión de la plantilla de inicialización.
5. En Auto Scaling guidance (Orientación sobre Auto Scaling), active la casilla de verificación para que Amazon EC2 proporcione orientación que le ayude a crear una plantilla para usarla con Auto Scaling.
6. Modifique los parámetros de inicialización según sea necesario. Debido a que ha seleccionado la orientación sobre Auto Scaling, algunos campos son obligatorios y otros no están disponibles. Para obtener más información sobre cómo configurar los parámetros de inicialización de Amazon EC2 Auto Scaling, consulte Create a launch template for an Auto Scaling group y Crear

una plantilla de inicialización mediante la configuración avanzada en la Guía del usuario de Amazon EC2 Auto Scaling.

7. Elija Crear plantilla de inicialización.
8. (Opcional) Para crear un grupo de escalado automático con esta plantilla de inicialización, en la página Next steps (Siguientes pasos) elija Create Auto Scaling group (Crear grupo de escalado automático).

Para ver ejemplos en los que se muestre cómo usar la AWS CLI para crear plantillas de inicialización con varias combinaciones de parámetros, consulte Examples for creating and managing launch templates with the AWS Command Line Interface (AWS CLI) en la Guía del usuario de Amazon EC2 Auto Scaling.

Para crear o actualizar un grupo de escalado automático con una plantilla de inicialización mediante la AWS CLI

- Utilice el comando create-auto-scaling-group o update-auto-scaling-group y especifique el parámetro `--launch-template`.

Para obtener más información sobre cómo crear o actualizar un grupo de escalado automático mediante una plantilla de inicialización, consulte los siguientes temas en la Guía del usuario de Amazon EC2 Auto Scaling.

- Create Auto Scaling groups using launch templates
- Update an Auto Scaling group

Usar plantillas de inicialización con flota de EC2

Puede crear una solicitud de flota de EC2 y especificar una plantilla de inicialización en la configuración de la instancia. Cuando Amazon EC2 atiende la solicitud de flota de EC2, utiliza los parámetros de inicialización definidos en la plantilla de inicialización asociada. Puede omitir algunos de los parámetros especificados en la plantilla de inicialización.

Para obtener más información, consulte Crear una flota de EC2.

Para crear una flota de EC2 con una plantilla de inicialización mediante la AWS CLI

- Utilice el comando create-fleet. Use el parámetro `--launch-template-configs` para especificar la plantilla de inicialización y cualquier otra omisión para la misma.

Usar plantillas de inicialización con la flota de spot

Puede crear una solicitud de flota de spot y especificar una plantilla de inicialización en la configuración de la instancia. Cuando Amazon EC2 atiende la solicitud de flota de spot, utiliza los parámetros de inicialización definidos en la plantilla de inicialización asociada. Puede omitir algunos de los parámetros especificados en la plantilla de inicialización.

Para obtener más información, consulte Creación de una solicitud de flota de spot.

Para crear una solicitud de flota de spot con una plantilla de inicialización mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Solicitudes de spot.
3. Elija Request Spot Instances (Solicitar instancias de spot).
4. En Launch parameters (Parámetros de inicialización), seleccione Use a launch template (Utilizar una plantilla de inicialización).
5. En Launch template (Plantilla de inicialización), elija una plantilla de inicialización y, a continuación, en el campo de la derecha, elija la versión de la plantilla de inicialización.
6. Para configurar su flota de spot, seleccione diferentes opciones en esta pantalla. Para obtener más información sobre las opciones, consulte Creación de una solicitud de flota de spot con los parámetros definidos (consola).
7. Cuando esté listo para crear su flota de spot, elija Launch (iniciar).

Para crear una solicitud de flota de spot con una plantilla de inicialización mediante la AWS CLI

- Utilice el comando request-spot-fleet. Use el parámetro `LaunchTemplateConfigs` para especificar la plantilla de inicialización y cualquier otra omisión para la misma.

inicialización de una instancia utilizando parámetros de una instancia existente

La consola de Amazon EC2 proporciona la opción Launch More Like This (iniciar más como esta) que le permite utilizar una instancia actual como base para iniciar otras instancias. Esta opción

rellena automáticamente el asistente de inicialización de instancias de Amazon EC2 con ciertos detalles de configuración de la instancia seleccionada.

Consideraciones

- No clonamos sus instancias; solo replicamos algunos de los detalles de configuración. Para crear una copia de la instancia, primero debe crear una AMI a partir de ella y, a continuación, iniciar otras instancias desde dicha AMI. Cree una plantilla de inicialización para asegurarse de iniciar sus instancias con los mismos detalles de inicialización.
- La instancia debe tener el estado `running`.

Detalles copiados

Los siguientes detalles de configuración se copian de la instancia seleccionada en el asistente de inicialización de instancias:

- ID de AMI
- Tipo de instancia
- Zona de disponibilidad, o la VPC y subred en la que se encuentra la instancia seleccionada
- Dirección IPv4 pública. Si la instancia seleccionada tiene actualmente una dirección IPv4 pública, la nueva instancia recibe una dirección IPv4 pública - con independencia de la configuración predeterminada de la dirección IPv4 pública de la instancia seleccionada. Para obtener más información acerca de las direcciones IPv4 públicas, consulte Direcciones IPv4 públicas.
- Grupo de ubicación, si procede
- Rol de IAM asociado a la instancia, si procede
- Ajustes del comportamiento de apagado (detenerse o terminar)
- Ajustes de protección de terminación (verdadero o falso)
- Monitorización de CloudWatch (habilitado o deshabilitado)
- Ajustes de optimización de Amazon EBS (verdadero o falso)
- Ajustes de tenencia, si se inicia en una VPC (compartida o dedicada)
- ID del kernel e ID del disco RAM, si procede
- Datos del usuario, si se especifican
- Etiquetas asociadas a la instancia, si procede
- Grupos de seguridad asociados a la instancia

- [Instancias de Windows] Información de asociación. Si la instancia seleccionada está asociada a un archivo de configuración, este se asocia automáticamente a la nueva instancia. Si el archivo de configuración incluye una configuración de dominio incorporado, la nueva instancia se incorpora al mismo dominio. Para obtener más información acerca de cómo unirse a un dominio, consulte Cómo unir fácilmente una instancia de EC2 de Windows en la Guía de administración de AWS Directory Service.

Detalles no copiados

Los siguientes detalles de configuración no se copian de la instancia seleccionada. En su lugar, el asistente aplica su configuración o comportamiento predeterminados:

- Número de interfaces de red: el valor predeterminado es una interfaz de red, la cual es la interfaz de red principal (eth0).
- Almacenamiento: los ajustes de almacenamiento predeterminados se determinan según la AMI y el tipo de instancia.

Cómo iniciar más instancias como una instancia existente

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Seleccione una instancia y elija Acciones, Imágenes y plantillas, iniciar más como esta.
4. Se abrirá el asistente de inicialización de instancias. Puede realizar los cambios que estime oportunos en la configuración de la instancia seleccionando diferentes opciones en esta pantalla.

   Cuando esté listo para iniciar su instancia, elija Launch Instance (iniciar instancia).
5. Si se produce un error al lanzar la instancia o el estado pasa inmediatamente a `terminated` en lugar de `running`, consulte Solucionar problemas de lanzamiento de instancias.

iniciar una AWS Marketplace instancia

Puede suscribirse a un producto de AWS Marketplace y iniciar una instancia desde la AMI del producto mediante el launch wizard de Amazon EC2. Para obtener más información acerca de las AMI pagadas, consulte AMI de pago. Para cancelar su suscripción después de la inicialización,

primero debe terminar todas las instancias que se ejecutan desde ella. Para obtener más información, consulte Administrar las suscripciones de AWS Marketplace.

New console

Para inicia una instancia desde AWS Marketplace con el launch wizard

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de la consola de Amazon EC2, elija iniciar instancia .
3. (Opcional) En Name and tags (Nombre y etiquetas), escriba un nombre descriptivo para la instancia en Name (Nombre).
4. En Imágenes de aplicaciones y sistema operativo (Imagen de máquina de Amazon), elija Buscar más AMI y, a continuación, elija la pestaña AMI de AWS Marketplace. Localice una AMI adecuada examinando las categorías o utilizando la funcionalidad de búsqueda. Elija Select (Seleccionar) para elegir un producto.
5. Aparecerá una ventana con información general del producto que haya seleccionado. Puede ver la información sobre precios, así como cualquier otra información que haya facilitado el proveedor. Cuando lo tenga todo listo, elija uno de los siguientes botones:
   - Suscribirse al iniciar una instancia: la suscripción comienza cuando elige iniciar instancia (en el paso 10).
   - Suscribirse ahora: la suscripción comienza inmediatamente. Mientras la suscripción esté en curso, puede seguir los pasos de este procedimiento para configurar la instancia. Si hay problemas con los datos de la tarjeta de crédito, se le pedirá que actualice los detalles de su cuenta.

   > **Note**
   >
   > No se le cobrará por utilizar el producto hasta que haya iniciado una instancia con la AMI. Tome nota del precio de cada tipo de instancia admitido cuando seleccione un tipo de instancia. También se podrían aplicar impuestos adicionales al producto.

6. En Instance type (Tipo de instancia), seleccione el tipo de instancia de la instancia. El tipo de instancia define la configuración de hardware y el tamaño de la instancia que se va a iniciar.
7. (Opcional) En Par de claves (inicio), para Nombre de par de claves seleccione un par de claves existente o cree uno nuevo.

8. En Network settings (Configuración de red), Firewall (security groups) (Firewall [grupos de seguridad]), tome nota del nuevo grupo de seguridad que se creó según las especificaciones del proveedor para el producto. El grupo de seguridad puede incluir reglas que permitan a todas las direcciones IPv4 (`0.0.0.0/0`) obtener acceso a SSH (puerto 22) en Linux o a RDP (puerto 3389) en Windows. Le recomendamos que ajuste esta reglas para permitir el acceso a la instancia a través de estos puertos únicamente a una dirección o a un rango de direcciones específico.
9. Puede usar los demás campos de la pantalla para configurar la instancia, agregar almacenamiento y etiquetas. Para obtener información acerca de las distintas opciones que puede configurar, consulte iniciar una instancia mediante parámetros definidos.
10. En el panel Summary (Resumen), en Software Image (AMI) (Imagen de software [AMI]), compruebe los detalles de la AMI desde la que va a iniciar la instancia. Compruebe también los demás detalles de configuración que haya especificado. Cuando lo tenga todo listo para iniciar una instancia, elija iniciar instancia.
11. Según el producto al que se haya suscrito, podrían transcurrir varios minutos antes de que la instancia se lance. Si eligió Suscribirse al iniciar una instancia en el paso 5, se suscribirá al producto antes de que se pueda iniciar la instancia. Si hay problemas con los datos de la tarjeta de crédito, se le pedirá que actualice los detalles de su cuenta. Cuando se muestre la página de confirmación de la inicialización, elija View all instances (Ver todas las instancias) para ir a la página Instances (instancia[s]).

> **Note**
>
> Se le cobrará el precio de suscripción siempre que la instancia esté en el estado `running`, incluso si está inactiva. Si se detiene la instancia, podría seguírsele cobrando por el almacenamiento.

12. Si la instancia tiene el estado `running`, no podrá conectarse a ella. Para ello, seleccione la instancia en la lista, elija Connect (Conectarse) y seleccione una opción de conexión. Para obtener más información sobre cómo conectarse a la instancia, consulte Conexión con la instancia de LinuxConexión con la instancia de Windows de.

> **Important**
>
> Lea detenidamente las instrucciones de uso del proveedor, ya que podría tener que utilizar un nombre de usuario específico para conectarse a la instancia. Para obtener

información acerca de cómo acceder a los detalles de la suscripción, consulte Administrar las suscripciones de AWS Marketplace.

13. Si se produce un error al iniciar la instancia o el estado pasa inmediatamente a `terminated` en lugar de `running`, consulte Solucionar problemas de lanzamiento de instancias.

Old console

Para inicia una instancia desde AWS Marketplace con el launch wizard

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de Amazon EC2, elija Launch Instance (iniciar instancia).
3. En la página Elegir una imagen de máquina de Amazon (AMI), elija la categoría AWS Marketplace que aparece a la izquierda. Localice una AMI adecuada buscando en las categorías o utilizando la funcionalidad de búsqueda. Elija Select (Seleccionar) para elegir el producto.
4. Aparecerá un cuadro de diálogo con información general del producto que ha seleccionado. Puede ver la información sobre precios, así como cualquier otra información que haya facilitado el proveedor. Cuando haya terminado, elija Continue (Continuar).

   > **Note**
   >
   > No se le cobrará por utilizar este producto hasta que haya iniciado una instancia con la AMI. Tome nota del precio de cada tipo de instancia admitido ya que se le pedirá que seleccione un tipo de instancia en la siguiente página del asistente. También se podrían aplicar impuestos adicionales al producto.

5. En la página Choose an Instance Type (Elegir un tipo de instancia), seleccione la configuración de hardware y el tamaño de la instancia que se va a iniciar. Cuando haya terminado, elija Next: Configure Instance Details (Siguiente: Configurar detalles de instancia).
6. En las páginas siguientes del asistente, podrá configurar la instancia y añadir almacenamiento y etiquetas. Para obtener más información acerca de las distintas opciones que puede configurar, consulte Lance una instancia con el antiguo asistente de inicialización de instancias. Elija Next hasta llegar a la página Configure Security Group.

   El asistente crea un nuevo grupo de seguridad según las especificaciones del producto del distribuidor. El grupo de seguridad puede incluir reglas para permitir a direcciones

IPv4 (`0.0.0.0/0`) obtener acceso a SSH (puerto 22) en Linux o a RDP (puerto 3389) en Windows. Le recomendamos que ajuste esta reglas para permitir el acceso a la instancia a través de estos puertos únicamente a una dirección o a un rango de direcciones específico.

Cuando esté listo, elija Review and Launch (Revisar y iniciar).

7. En la página Review Instance Launch (Revisar inicialización de instancia), compruebe los detalles de la AMI desde la que va a iniciar la instancia, así como los demás detalles de configuración que configuró a través del asistente. Cuando esté listo, elija Launch (iniciar) para seleccionar o crear un par de claves y iniciar la instancia.
8. Dependiendo del producto al que se haya suscrito, podrían transcurrir varios minutos antes de que la instancia se lance. Debe suscribirse al producto antes de que se pueda iniciar la instancia. Si hay problemas con los datos de la tarjeta de crédito, se le pedirá que actualice los detalles de su cuenta. Cuando se muestra la página de confirmación de la inicialización, elija View Instances (Ver instancias) para ir a la página de instancias.

> **Note**
>
> Se le cobrará el precio de la suscripción siempre que la instancia esté en ejecución, incluso si está inactiva. Si se detiene la instancia, podrían seguírsele cobrando por el almacenamiento.

9. Si la instancia tiene el estado `running`, no podrá conectarse a ella. Para ello, seleccione la instancia en la lista y elija Connect (Conectarse). Siga las instrucciones que se detallan en el cuadro de diálogo. Para obtener más información sobre cómo conectarse a la instancia, consulte Conexión con la instancia de LinuxConexión con la instancia de Windows de.

> **Important**
>
> Lea detenidamente las instrucciones de uso del proveedor, ya que podría tener que utilizar un nombre de usuario específico para iniciar sesión en la instancia. Para obtener más información sobre cómo obtener acceso a los detalles de la suscripción, consulte Administrar las suscripciones de AWS Marketplace.

10. Si se produce un error al iniciar la instancia o el estado pasa inmediatamente a `terminated` en lugar de `running`, consulte Solucionar problemas de lanzamiento de instancias.

iniciar una AWS Marketplace instancia de AMI mediante API y CLI

Para iniciar instancias desde productos de AWS Marketplace mediante la API o y herramientas de líneas de comando, primero asegúrese de estar suscrito al producto. A continuación, podrá iniciar una instancia con el ID de la AMI del producto siguiendo los siguientes métodos:

Método	Documentación
AWS CLI	Utilice el comando run-instances o consulte el siguiente tema para obtener más información: inicialización de una instancia.
AWS Tools for Windows PowerShell	Utilice el comando New-EC2Instance o consulte el siguiente tema para obtener más información: inicialización de una instancia Amazon EC2 mediante Windows PowerShell
API de consulta	Utilice la solicitud RunInstances.

Detención e iniciación de una instancia de Amazon EC2

Puede detener e iniciar la instancia si tiene un volumen de Amazon EBS como dispositivo raíz. Cuando se detiene una instancia, esta se cierra. Al iniciar una instancia, esta suele migrarse a un nuevo equipo host subyacente y se le asigna una nueva dirección IPv4 pública.

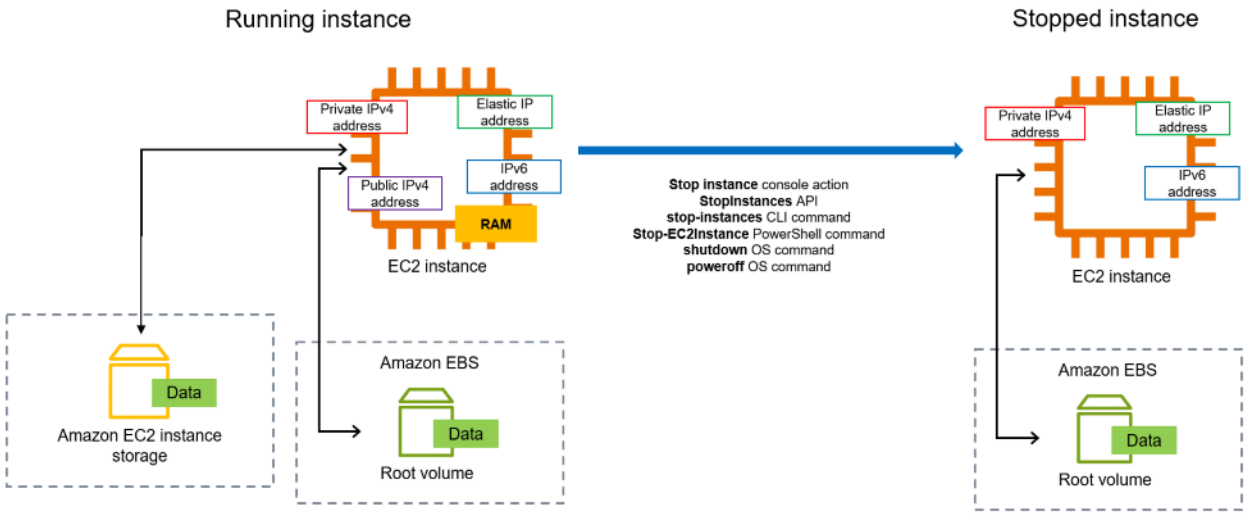
Cuando detiene una instancia, no se elimina. Si decide que ya no necesita una instancia, puede terminarla. Para obtener más información, consulte Terminación de las instancias de Amazon EC2. Si desea poner en hibernación una instancia para guardar el contenido de la memoria de la instancia (RAM), consulte Hibernación de la instancia de Amazon EC2. Para ver las distinciones entre las acciones del ciclo de vida de la instancia, consulte Diferencias entre reinicio, detención, hibernación y terminación.

Contenido

Cómo funciona la detención y el inicio de instancias

Cuando se detiene una instancia, los cambios se registran en el nivel de SO de la instancia, algunos recursos se pierden y otros persisten. Al iniciar una instancia, los cambios se registran a nivel de instancia.

El siguiente diagrama muestra lo que se pierde y lo que persiste cuando se detiene una instancia de Amazon EC2. Cuando una instancia se detiene, pierde todos los volúmenes del almacén de instancias adjuntos y los datos almacenados en esos volúmenes, los datos almacenados en la RAM de la instancia y la dirección IPv4 pública asignada si no hay una dirección IP elástica asociada a la instancia. Una instancia conserva las direcciones IPv4 privadas asignadas, las direcciones IP elásticas asociadas a la instancia, cualquier dirección IPv6 y cualquier volumen de Amazon EBS adjunto, así como los datos de esos volúmenes.



Qué ocurre cuando se detiene una instancia

Cambios registrados a nivel del SO

- La solicitud de la API envía un evento de pulsación de botón al invitado.
- Hay varios servicios del sistema que se detienen como resultado del evento de pulsación del botón. El apagado estable se activa desde el hipervisor a través del evento de pulsación del botón de apagado de ACPI.
- Se inicia el apagado de ACPI.
- La instancia se apaga cuando se termina el proceso de apagado estable. El tiempo de apagado del SO no puede configurarse.

- Si el sistema operativo de la instancia no se cierra correctamente en cuatro minutos, se realiza un cierre completo.
- La instancia deja de ejecutarse.
- El estado de la instancia cambia a `stopping` y, a continuación, a `stopped`.
- Escalado automático Si la instancia está en un grupo de escalado automático, cuando la instancia se encuentre en cualquier estado de Amazon EC2 distinto de `running` o si el estado de las comprobaciones de estado se vuelve `impaired`, Amazon EC2 Auto Scaling considera que la instancia está en mal estado y la reemplaza. Para obtener más información, consulte Comprobaciones de estado de las instancias de escalado automático en la guía del usuario de Amazon EC2 Auto Scaling.
- [Instancias de Windows] Al detener e iniciar una instancia de Windows, el agente de inicialización realiza ciertas tareas en la instancia, como cambiar las letras de unidad de los volúmenes de Amazon EBS adjuntos. Para obtener más información acerca de estos valores predeterminados y de cómo puede cambiarlos, consulte the section called “EC2Launch v2”.

Recursos perdidos

- Datos almacenados en la memoria RAM.
- Datos almacenados en los volúmenes del almacén de instancias.
- La dirección IPv4 pública que Amazon EC2 asignó a la instancia de forma automática en el momento de iniciarla o iniciarla. Para retener una dirección IPv4 pública que no cambie nunca, puede asociar una dirección IP elástica a su instancia.

Recursos que persisten

- Cualquier volumen de Amazon EBS adjunto.
- Datos almacenados en los volúmenes de Amazon EBS adjuntos.
- Direcciones IPv4 privadas
- Direcciones IPv6
- Direcciones IP elásticas asociadas a la instancia Tenga en cuenta que, cuando la instancia se detiene, se le comenzará a cobrar las direcciones IP elásticas asociadas.

Para obtener más información acerca de qué sucede cuando detiene una instancia de Mac, consulte the section called “Detener y finalizar la instancia de Mac”.

Qué ocurre cuando se detiene una instancia

Cambios registrados a nivel del SO

- En la mayoría de los casos, la instancia se migra a una nueva computadora host subyacente (aunque, en algunos casos, como cuando una instancia se asigna a un host en una configuración de host dedicado permanece en el host actual).
- Amazon EC2 asigna una nueva dirección IPv4 pública a la instancia si esta se configura para recibir una dirección IPv4 pública. Para retener una dirección IPv4 pública que no cambie nunca, puede asociar una dirección IP elástica a su instancia.

Probar la respuesta de la aplicación a la detención y el inicio

Puede usar AWS Fault Injection Service para probar cómo responde la aplicación cuando la instancia se interrumpe y se inicia. Para obtener más información, consulte la Guía del usuario de AWS Fault Injection Service.

Costos relacionados con el inicio y la detención de una instancia

Los siguientes costos están asociados a la detención e inicio de una instancia.

Detención: tan pronto como el estado de una instancia cambie a `shutting-down` o `terminated`, ya no se incurrirán en cargos por la instancia. No se le cobrarán comisiones por uso ni por transferencia de datos por una instancia detenida. Se incurre en cargos por almacenar los volúmenes de almacenamiento de Amazon EBS.

Inicio: cada vez que inicie una instancia detenida, se le cobrará un cargo mínimo de un minuto de uso. Después del primer minuto, solo le cobramos los segundos que utilice. Por ejemplo, si ejecuta una instancia durante 20 segundos y luego la detiene, se le cobrará un minuto de uso completo. Si ejecuta una instancia durante 3 minutos y 40 segundos, se le cobrarán 3 minutos y 40 segundos de uso.

Detención e inicio de sus instancias de forma manual

Puede detener e iniciar las instancias con respaldo de Amazon EBS (instancias con dispositivos raíz de EBS). No se pueden detener e iniciar instancias con el dispositivo raíz del almacén de instancias.

> **Warning**
>
> Cuando detiene una instancia, se borran los datos contenidos en todos los volúmenes de almacén de instancias. Antes de detener una instancia, compruebe que ha copiado todos los datos que necesita de los volúmenes del almacén de instancias al almacenamiento persistente, como Amazon EBS o Amazon S3.

Console

Detención e inicio de una instancia respaldada por Amazon EBS

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación izquierdo, seleccione Instancias y, a continuación, seleccione la instancia.
3. En la pestaña Almacenamiento, compruebe que el tipo de dispositivo raíz sea EBS. De lo contrario, no podrá detener la instancia.
4. Elija Instance state (Estado de la instancia) y Stop instance (Detener instancia). Si esta opción está desactivada, la instancia ya está detenida o bien su dispositivo raíz es un volumen de almacén de instancias.
5. Cuando se le pida que confirme, elija Stop. Puede que transcurran unos minutos hasta que la instancia se detenga.
6. Para iniciar una instancia detenida, seleccione la instancia y elija Estado de la instancia e Iniciar instancia.
7. Puede que transcurran unos minutos hasta que la instancia pase al estado `running`.
8. Si detiene una instancia respaldada por Amazon EBS y aparece como “bloqueada” en el estado `stopping`, puede forzar su detención. Para obtener más información, consulte Solucionar problemas de detención de la instancia.

Command line

Requisitos previos

Compruebe que el dispositivo raíz de la instancia sea un volumen de EBS. Por ejemplo, ejecute el comando de la AWS CLI describe-instances y compruebe que el `RootDeviceType` sea `ebs` y no `instance-store`.

Detención e inicio de una instancia respaldada por Amazon EBS

Utilice uno de los siguientes comandos:

- AWS CLI:stop-instances y start-instances.
- AWS Tools for PowerShell:Stop-EC2Instance y Start-EC2Instance.
- Comandos del sistema operativo: puede iniciar un apagado mediante los comandos shutdown o poweroff. Cuando utiliza un comando del sistema operativo, la instancia se detiene de forma predeterminada. Puede cambiar este comportamiento para que se termine. Para obtener más información, consulte Cambiar el comportamiento de apagado iniciado por la instancia.

[Instancias de Linux] El uso del comando halt del sistema operativo en una instancia no inicia un apagado. Si usa el comando halt, la instancia no termina, sino que coloca la CPU en HLT, lo que suspende el funcionamiento de la CPU. La instancia permanece en el estado de ejecución.

Detener e iniciar sus instancias de forma automática

Puede automatizar la detención y el inicio de las instancias con los siguientes servicios:

El programador de instancias en AWS

Puede utilizar el programador de instancias en AWS para automatizar el inicio y la detención de instancias de EC2. Para obtener más información, consulte How do I use Instance Scheduler with CloudFormation to schedule EC2 instances? (¿Cómo usar el programador de instancias con CloudFormation para programar instancias de EC2?) Tenga en cuenta que se aplican cargos adicionales.

AWS Lambda y una regla de Amazon EventBridge

Puede utilizar Lambda y una regla de EventBridge para detener e iniciar las instancias según un cronograma. Para obtener más información, consulte ¿Cómo puedo utilizar la función de Lambda para detener e iniciar las instancias de Amazon EC2 a intervalos regulares?

Amazon EC2 Auto Scaling

Para asegurarse de que dispone del número correcto de instancias de Amazon EC2 para gestionar la carga de una aplicación, cree grupos de escalado automático. Amazon EC2 Auto Scaling garantiza que su aplicación siempre tenga la capacidad adecuada para manejar la demanda de tráfico y ahorra costos al iniciar instancias solo cuando es necesario. Tenga en

cuenta que Amazon EC2 Auto Scaling termina, en lugar de detener, las instancias innecesarias. Para configurar grupos de escalado automático, consulte Introducción a Amazon EC2 Auto Scaling.

Búsqueda de todas las instancias en ejecución y detenidas

Puede encontrar todas las instancias en ejecución y detenidas en todas las Regiones de AWS en una sola página en Amazon EC2 Global View. Esta capacidad resulta particularmente práctica para hacer un inventario y encontrar las instancias olvidadas. Para obtener información acerca de cómo utilizar Global View, consulte Amazon EC2 Global View.

Habilitación de la protección de detención para su instancia

Para evitar que una instancia se detenga de forma accidental, puede habilitar la protección de detención para la instancia. La protección de detención también protege la instancia de una terminación accidental.

El atributo `DisableApiStop` de la API `ModifyInstanceAttribute` de Amazon EC2 controla si la instancia se puede detener mediante la consola de Amazon EC2, la AWS CLI o la API de Amazon EC2. Puede establecer el valor de este atributo cuando inicia la instancia, mientras la instancia se encuentre en ejecución o cuando está detenida.

Consideraciones

- La protección contra detención no evita que detenga accidentalmente una instancia cuando comienza el cierre desde la instancia con un comando del sistema operativo, como shutdown o poweroff.
- La habilitación de la protección contra detención no impide que AWS detenga la instancia cuando hay un evento programado para detener la instancia.
- La habilitación de la protección de detención no impide que Amazon EC2 Auto Scaling termine una instancia cuando la instancia no está en buen estado o durante eventos de reducción horizontal. Es posible controlar si un grupo de escalado automático puede terminar una instancia concreta durante la reducción horizontal al utilizar la protección frente a la reducción horizontal de instancias.
- La protección de detención no solo evita que la instancia se detenga accidentalmente, sino que también evita una terminación accidental cuando se utiliza la consola, la AWS CLI o la API. Sin embargo, no configura de manera automática el atributo `DisableApiTermination`. Tenga en cuenta que cuando el atributo `DisableApiStop` se establece en `false`, el

atributo `DisableApiTermination` se usa para determinar si la instancia se puede terminar mediante la consola, la AWS CLI o la API. Para obtener más información, consulte Terminación de las instancias de Amazon EC2.

- No puede habilitar la protección contra detención para instancias respaldadas por el almacén de instancias.
- No puede habilitar la protección contra detención para instancias de spot.
- La API de Amazon EC2 sigue un modelo de coherencia final cuando habilita o deshabilita la protección de detención. Esto significa que es posible que el resultado de ejecutar comandos para establecer el atributo de protección contra la detención no esté inmediatamente visible para todos los comandos posteriores que ejecute. Para obtener más información, consulte Consistencia eventual en la Guía para desarrolladores de Amazon EC2.

Acciones de protección contra detención

- Habilitar la protección de detención para una instancia en la inicialización
- Para habilitar la protección de detención para una instancia en ejecución o detenida
- Deshabilitar la protección de detención para una instancia en ejecución o detenida

Habilitar la protección de detención para una instancia en la inicialización

Puede habilitar la protección de detención para una instancia en la inicialización mediante uno de los métodos a continuación.

Console

Para habilitar la protección de detención para una instancia en la inicialización

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel, elija iniciar instancia.
3. Configure la instancia en el nuevo asistente de inicialización de instancias.
4. Para habilitar la protección de detención, elija Habilitar para Protección de detención dentro de Detalles avanzados en el asistente.

AWS CLI

Para habilitar la protección de detención para una instancia en la inicialización

Utilice el comando run-instances (Ejecutar instancias) de la AWS CLI para iniciar la instancia y especifique el parámetro `disable-api-stop`.

```
aws ec2 run-instances \
    --image-id ami-a1b2c3d4e5example \
    --instance-type t3.micro \
    --key-name MyKeyPair \
    --disable-api-stop \
    ...
```

Para habilitar la protección de detención para una instancia en ejecución o detenida

Puede habilitar la protección de detención para una instancia mientras se encuentre en ejecución o detenida mediante uno de los métodos a continuación.

Console

Para habilitar la protección de detención para una instancia en ejecución o detenida

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación izquierdo, elija instancias.
3. Seleccione la instancia y, a continuación, elija Acciones>Configuración de la instancia>Cambiar protección de detención.
4. Seleccione la casilla de verificación Enable (Habilitar) y, luego, elija Save (Guardar).

AWS CLI

Para habilitar la protección de detención para una instancia en ejecución o detenida

Utilice el comando modify-instance-attribute de la AWS CLI y especifique el parámetro `disable-api-stop`.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --disable-api-stop
```

Deshabilitar la protección de detención para una instancia en ejecución o detenida

Puede deshabilitar la protección de detención para una instancia en ejecución o detenida mediante uno de los métodos a continuación.

Console

Deshabilitar la protección de detención para una instancia en ejecución o detenida

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación izquierdo, elija instancias.
3. Seleccione la instancia y, a continuación, elija Actions (Acciones), Instance Settings (Configuración de instancia), Change Stop Protection (Cambiar protección de detención).
4. Desactive la casilla de verificación Habilitar y, luego, elija Guardar.

AWS CLI

Deshabilitar la protección de detención para una instancia en ejecución o detenida

Utilice el comando modify-instance-attribute de la AWS CLI y especifique el parámetro `no-disable-api-stop`.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --no-disable-api-stop
```

Hibernación de la instancia de Amazon EC2

Cuando hiberna una instancia, Amazon EC2 señala el sistema operativo que realice la hibernación (suspensión a disco). La hibernación guarda el contenido de la memoria de la instancia (RAM) en su volumen raíz de Amazon Elastic Block Store (Amazon EBS). Amazon EC2 conserva el volumen raíz de EBS de la instancia y cualquier volumen de datos de EBS adjunto. Cuando se inicie la instancia:

- El volumen raíz de EBS se restaura a su estado anterior
- El contenido de la RAM se volverá a cargar
- Se reanudarán los procesos que se estaban ejecutando anteriormente en la instancia
- Los volúmenes de datos que estaban adjuntos previamente se vuelven a adjuntar y la instancia conserva su ID de instancia

Puede hibernar una instancia solo si está habilitada para la hibernación y cumple los requisitos previos de hibernación.

Si una instancia o aplicación tarda mucho tiempo en arrancar y crear una huella de memoria para ser totalmente productiva, puede utilizar la hibernación para “precalentar” la instancia. Para “precalentar” la instancia:

1. Láncela con la hibernación habilitada.
2. Póngala en un estado deseado.
3. Hibérnela para que esté lista para reanudarse al estado deseado cuando sea necesario.

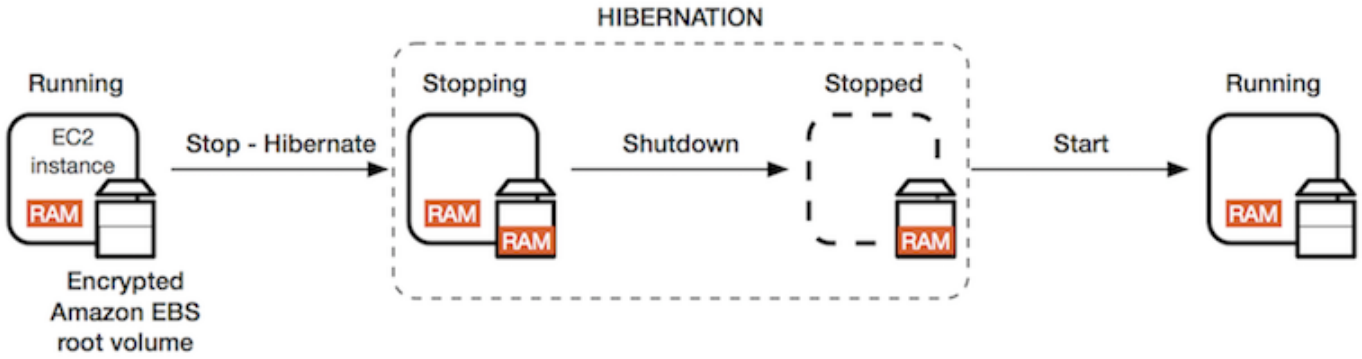
No se le cobra por el uso de una instancia en hibernación cuando está en el estado `stopped` o por la transferencia de datos cuando el contenido de la RAM se transfiere al volumen raíz de EBS. Se le cobra por el almacenamiento de cualquier volumen de EBS, incluido el almacenamiento del contenido de la RAM.

Si ya no necesita una instancia, puede terminarla en cualquier momento, incluso si está en el estado `stopped` (hibernado). Para obtener más información, consulte Terminación de las instancias de Amazon EC2.

Contenido

Cómo funciona la hibernación de instancias de Amazon EC2

En el siguiente diagrama, se muestra un resumen básico del proceso de hibernación para instancias de EC2.



¿Qué ocurre cuando se hiberna una instancia?

Cuando se hiberna una instancia, ocurre lo siguiente:

- La instancia cambia al estado `stopping`. Amazon EC2 señala al sistema operativo que realice la hibernación (suspensión a disco). La hibernación bloquea todos los procesos, guarda el contenido de la RAM en el volumen raíz de EBS y, a continuación, realiza un apagado normal.
- Una vez que se ha completado el apagado, la instancia pasa al estado `stopped`.
- Los volúmenes de EBS siguen asociados a la instancia y sus datos continúan, incluido el contenido guardado de la RAM.
- Los volúmenes del almacén de instancias de Amazon EC2 permanecen asociados a la instancia, pero los datos de estos volúmenes se pierden.
- Mientras la estancia está en estado `stopped`, puede modificar ciertos atributos de esta, incluido el tipo o tamaño de la instancia.
- En la mayoría de los casos, la instancia se migra a un nuevo equipo host subyacente al iniciarse. Es lo mismo que ocurre cuando detiene e inicia una instancia.
- Cuando se inicie la instancia, esta arranca y el sistema operativo lee el contenido de la RAM del volumen raíz de EBS antes de desbloquear los procesos para reanudar su estado.
- La instancia conserva sus direcciones IPv4 privadas y cualquier dirección IPv6. Al iniciar la instancia, la instancia continúa conservando sus direcciones IPv4 privadas y cualquier dirección IPv6.
- Amazon EC2 libera la dirección IPv4 pública. Al iniciar la instancia, Amazon EC2 asigna una nueva dirección IPv4 pública a la instancia.
- La instancia conserva sus direcciones IP elásticas asociadas. Se le cobrarán aquellas direcciones IP elásticas asociadas a una instancia hibernada.

Para obtener información acerca de las diferencias entre la hibernación y el reinicio, la detención y la terminación, consulte Diferencias entre reinicio, detención, hibernación y terminación.

Limitaciones

- Cuando una instancia se pone en hibernación, se pierden los datos de todos los volúmenes del almacén de instancias.
- (instancias de Linux) No puede poner en hibernación una instancia de Linux que tenga más de 150 GB de RAM.
- (instancias de Windows) No puede poner en hibernación una instancia de Windows que tenga más de 16 GB de RAM.
- Si crea una instantánea o AMI desde una instancia que está hibernada o tiene habilitada la hibernación, es posible que no pueda conectarse a una nueva instancia que se lance desde la AMI o desde una AMI que se haya creado desde la instancia.
- (Solo instancias de spot) Si Amazon EC2 pone a hibernar su instancia de spot, solo Amazon EC2 podrá reanudarla. Si poner a hibernar su instancia de spot (hibernación iniciada por el usuario), puede reanudarla. Una instancia de spot en hibernación solo se puede reanudar si hay capacidad disponible y el precio de spot es menor o igual que el precio máximo especificado.
- No puede hibernar una instancia que esté en un grupo de Auto Scaling o esté siendo utilizada por Amazon ECS. Si la instancia está en un grupo de Auto Scaling e intenta que hiberne, el servicio Amazon EC2 Auto Scaling marca la instancia detenida como instancia en mal estado, y puede terminarla y iniciar una instancia de sustitución. Para obtener más información, consulte Comprobaciones de estado para instancias en un grupo de escalado automático en la Guía del usuario de Amazon EC2 Auto Scaling.
- No puede hibernar una instancia que esté configurada para arrancar en modo UEFI con la opción Arranque seguro UEFI habilitada.
- Si hiberna una instancia que se lanzó en un Reserva de capacidad, el Reserva de capacidad no garantiza que la misma pueda reanudarse después de intentar iniciarla.
- No puede poner en hibernación una instancia que utilice un núcleo inferior a la versión 5.10 si está activado el modo estándar federal de procesamiento de información (FIPS).
- No se admite la hibernación de una instancia durante más de 60 días. Para mantener la instancia durante más de 60 días, debe iniciar la instancia hibernada, detener la instancia e iniciarla.
- Actualizamos constantemente nuestra plataforma con mejoras y parches de seguridad, que pueden entrar en conflicto con las instancias hibernadas existentes. Le informaremos acerca de las actualizaciones críticas que requieran un inicio de las instancias hibernadas, de manera

que podamos realizar un apagado o un reinicio para aplicar las actualizaciones y los parches de seguridad necesarios.

Consideraciones a la hora de hibernar una instancia de spot

- Si pone a hibernar su instancia de spot, puede reiniciarla siempre que haya capacidad disponible y el precio de spot sea menor o igual que el precio máximo especificado.
- Si Amazon EC2 pone a hibernar su instancia de spot:
  - Solo Amazon EC2 puede reanudar la instancia.
  - Amazon EC2 reanuda la instancia de spot en hibernación tan pronto como haya capacidad disponible con un precio de spot menor o igual que el precio máximo especificado.
  - Antes de que Amazon EC2 ponga a hibernar su instancia de spot, recibirá un aviso de interrupción dos minutos antes de que comience la hibernación.

  Para obtener más información, consulte Interrupciones de instancias de spot.
- Hay varias formas de habilitar la hibernación de una instancia de spot. Para obtener más información, consulte Especificar el comportamiento de interrupción.

Requisitos previos para la hibernación de instancias de Amazon EC2

Puede habilitar el soporte de hibernación para una instancia bajo demanda o una instancia de spot al iniciarla. No se puede habilitar la hibernación en una instancia existente, independientemente de si está en ejecución o detenida. Para obtener más información, consulte Habilitación de la hibernación de una instancia.

Requisitos de hibernación de una instancia

- Regiones de AWS
- AMI
- Familias de instancias
- Tamaño de RAM de instancia
- Tipo de volumen raíz
- Tamaño del volumen raíz
- Cifrado de volumen raíz
- Tipo de volumen de EBS

- Solicitudes de instancia de spot

Regiones de AWS

Puede usar la hibernación con instancias en todas las Regiones de AWS.

AMI

Debe utilizar una AMI de HVM compatible con la hibernación. Las siguientes AMI admiten la hibernación:

AMI de Linux

- AMI de AL2023 iniciada el 20/09/2023 o posteriormente.
- AMI de Amazon Linux 2 iniciada el 29/08/2019 o posteriormente
- AMI de Amazon Linux 2018.03 lanzada el 16/11/2018 o posteriormente
- AMI de CentOS versión 8 [1] (la configuración adicional es obligatoria)
- AMI de Fedora versión 34 o posterior [1] (la configuración adicional es obligatoria)
- AMI de Red Hat Enterprise Linux (RHEL) 9 [1] (la configuración adicional es obligatoria)
- AMI de Red Hat Enterprise Linux (RHEL) 8 [1] (la configuración adicional es obligatoria)
- AMI de Ubuntu 22.04.2 LTS (Jammy Jellyfish) iniciada con el número de serie 20230303 o uno posterior [2]
- AMI de Ubuntu 20.04 LTS (Focal Fossa) iniciada con el número de serie 20210820 o posterior [2]
- AMI de Ubuntu 18.04 LTS (Bionic Beaver) iniciada con el número de serie 20190722.1 o posterior [2] [4]
- AMI de Ubuntu 16.04 LTS (Xenial Xerus) [2] [3] [4] (la configuración adicional es obligatoria)

[1] Para CentOS, Fedora y Red Hat Enterprise Linux, solo se admite la hibernación en instancias basadas en Nitro.

[2] Recomendamos deshabilitar KASLR en instancias con Ubuntu 22.04.2 LTS (Jammy Jellyfish), Ubuntu 20.04 LTS (Focal Fossa), Ubuntu 18.04 LTS (Bionic Beaver) y Ubuntu 16.04 LTS (Xenial Xerus). Para obtener más información, consulte Deshabilitación de KASLR en una instancia (solo Ubuntu).

[3] Para la AMI de Ubuntu 16.04 LTS (Xenial Xerus), la hibernación no se admite en los tipos de instancias `t3.nano`. No habrá ninguna revisión disponible porque Ubuntu (Xenial Xerus) finalizó el soporte en abril de 2021. Si desea utilizar los tipos de instancia `t3.nano`, le recomendamos que actualice a la AMI de Ubuntu 22.04.2 LTS (Jammy Jellyfish), Ubuntu 20.04 LTS (Focal Fossa) o la AMI de Ubuntu 18.04 LTS (Bionic Beaver).

[4] El soporte para Ubuntu 18.04 LTS (Bionic Beaver) y Ubuntu 16.04 LTS (Xenial Xerus) ha llegado al final de su vida útil.

Para configurar su propia AMI para admitir la hibernación, consulte Configuración de una AMI de Linux para que admita la hibernación.

Se ofrecerá soporte para otras versiones de Ubuntu y otros sistemas operativos próximamente.

AMI de Windows

- AMI de Windows Server 2022 iniciada el 13/09/2023 o posteriormente
- AMI de Windows Server 2019 iniciada el 11/09/2019 o posteriormente
- AMI de Windows Server 2016 iniciada el 11/09/2019 o posteriormente
- AMI de Windows Server 2012 R2 iniciada el 11/09/2019 o posteriormente
- AMI de Windows Server 2012 iniciada el 11/09/2019 o posteriormente

Familias de instancias

Debe usar una familia de instancias que admita la hibernación.

- De uso general: M3, M4, M5, M5a, M5ad, M5d, M6i, M6id, M7i, M7i-flex, T2, T3, T3a
- Optimizadas para la computación: C3, C4, C5, C5d, C6i, C6id, C7a, C7i, C7i-flex
- Optimizadas para la memoria: R3, R4, R5, R5a, R5ad, R5d, R7a, R7i, R7iz
- Optimizadas para el almacenamiento: I3, I3en

instancias de Nitro: no se admiten instancias bare metal.

Para ver los tipos de instancias disponibles que son compatibles con la hibernación en una región específica

Los tipos de instancia disponibles varían según la región. Para ver los tipos de instancias disponibles que son compatibles con la hibernación en una región, utilice el comando describe-instance-types

con el parámetro `--region`. Incluya el parámetro `--filters` a fin de limitar los resultados a los tipos de instancia que admiten la hibernación y el parámetro `--query` para limitar la salida al valor de `InstanceType`.

```
aws ec2 describe-instance-types --filters Name=hibernation-supported,Values=true --
query "InstanceTypes[*].[InstanceType]" --output text | sort
```

Ejemplo de resultado

```
c3.2xlarge
c3.4xlarge
c3.8xlarge
c3.large
c3.xlarge
c4.2xlarge
c4.4xlarge
c4.8xlarge
...
```

Tamaño de RAM de instancia

instancias de Linux: deben ser inferiores a 150 GB.

instancias de Windows: pueden tener un tamaño de hasta 16 GB. Para hibernar una instancia T3 o T3a de Windows, recomendamos al menos 1 GB de RAM.

Tipo de volumen raíz

El volumen raíz debe ser un volumen de EBS, no un volumen de almacén de instancias.

Tamaño del volumen raíz

El tamaño del volumen raíz debe ser lo suficientemente grande como para almacenar el contenido de la RAM y adaptarse al uso esperado, por ejemplo, del SO o de las aplicaciones. Si habilita la hibernación, se asigna espacio en el volumen raíz en el momento de la inicialización para almacenar la RAM.

Cifrado de volumen raíz

Debe cifrarse el volumen raíz a fin de garantizar la protección del contenido confidencial que se encuentre en la memoria en el momento de la hibernación. Cuando los datos de la RAM pasan al

volumen raíz de EBS, siempre se cifran. El cifrado del volumen raíz es obligatorio en el momento de la inicialización de la instancia.

Utilice una de las tres opciones siguientes para asegurarse de que el volumen raíz es un volumen de EBS cifrado:

- Cifrado de EBS de forma predeterminada: puede habilitar el cifrado de EBS de forma predeterminada para asegurarse de que se cifren todos los volúmenes de EBS nuevos creados en su cuenta de AWS. De esta forma, puede habilitar la hibernación en sus instancias sin especificar el intento de cifrado al iniciar la instancia. Para obtener más información, consulte Habilitación del cifrado de manera predeterminada.
- Cifrado de EBS de un “solo paso”: puede iniciar instancias de EC2 respaldadas por EBS cifradas a partir de una AMI sin cifrado y a la vez habilitar la hibernación. Para obtener más información, consulte Usar el cifrado con las AMI con respaldo de EBS.
- AMI cifrada: puede habilitar el cifrado de EBS con una AMI cifrada para iniciar su instancia. Si su AMI no tiene una instantánea raíz cifrada, puede copiarla a una nueva AMI y solicitar su cifrado. Para obtener más información, consulte Cifrar una imagen sin cifrar durante la copia y Copiar una AMI.

Tipo de volumen de EBS

Los volúmenes de EBS deben utilizar alguno de los siguientes tipos de volumen de EBS:

- SSD de uso general (`gp2` y `gp3`)
- SSD de IOPS provisionadas (`io1` y `io2`)

Si elige un tipo de volumen de SSD de IOPS provisionadas, debe aprovisionar el volumen de EBS con las IOPS adecuadas a fin de lograr un rendimiento óptimo para la hibernación. Para obtener más información, consulte Tipos de volúmenes de Amazon EBS en la Guía del usuario de Amazon EBS.

Solicitudes de instancia de spot

Para las instancias de spot, se aplican los siguientes requisitos:

- El tipo de solicitud de instancia de spot: debe ser `persistent`.
- No puede especificar un grupo de inicialización en la solicitud de instancia de spot.

Configuración de una AMI de Linux para que admita la hibernación

Las siguientes AMI de Linux admiten la hibernación, pero, para hibernar una instancia que se lanzó con una de estas AMI, se requiere una configuración adicional a fin de poder hibernar la instancia.

Se requiere configuración adicional para:

- AMI mínima de Amazon Linux 2 iniciada el 29/08/2019 o posteriormente
- Amazon Linux 2 iniciado antes del 29/08/2019
- Amazon Linux lanzado antes del 16/11/2018
- CentOS, versión 8 o posterior
- Fedora, versión 34 o posterior
- Red Hat Enterprise Linux, versión 8 o 9
- Ubuntu 20.04 LTS (Focal Fossa) iniciado antes del número de serie 20210820
- Ubuntu 18.04 (Bionic Beaver) iniciado con el número de serie 20190722.1
- Ubuntu 16.04 (Xenial Xerus)

Para obtener más información, consulte Actualización de software en la instancia de Amazon Linux 2.

No se requieren configuraciones adicionales para las siguientes AMI porque ya se encuentran configuradas a fin de admitir la hibernación:

- AMI de AL2023 iniciada el 20/09/2023 o posteriormente.
- AMI completa de Amazon Linux 2 iniciada el 29/08/2019 o posteriormente
- AMI de Amazon Linux 2018.03 iniciada el 16/11/2018 o posteriormente
- AMI de Ubuntu 22.04.2 LTS (Jammy Jellyfish) iniciada con el número de serie 20230303 o uno posterior
- AMI de Ubuntu 20.04 LTS (Focal Fossa) iniciada con el número de serie 20210820 o posterior
- AMI de Ubuntu 18.04 LTS (Bionic Beaver) iniciada con el número de serie 20190722.1 o posterior

AMI mínima de Amazon Linux 2 iniciada el 29/08/2019 o posteriormente

Para configurar una AMI mínima de Amazon Linux 2 iniciada el 29/08/2019 o posteriormente a fin de que sea compatible con la hibernación

1. Instale el paquete `ec2-hibinit-agent` de los repositorios.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

2. Reinicie el servicio .

```
[ec2-user ~]$ sudo systemctl start hibinit-agent
```

Amazon Linux 2 iniciado antes del 29/08/2019

Para configurar una AMI de Amazon Linux 2 iniciada antes del 29/08/2019 a fin de que sea compatible con la hibernación

1. Actualice el kernel a la versión `4.14.138-114.102` o posterior.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Instale el paquete `ec2-hibinit-agent` de los repositorios.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

3. Reinicie la instancia.

```
[ec2-user ~]$ sudo reboot
```

4. Confirme que la versión del kernel se ha actualizado a la versión `4.14.138-114.102` o posterior.

```
[ec2-user ~]$ uname -a
```

5. Detenga la instancia y cree una AMI. Para obtener más información, consulte Creación de una AMI basada en Amazon EBS.

Amazon Linux lanzado antes del 16/11/2018

Para configurar una AMI de Amazon Linux iniciada antes del 16/11/2018 a fin de que sea compatible con la hibernación

1. Actualice el kernel a la versión `4.14.77-70.59` o posterior.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Instale el paquete `ec2-hibinit-agent` de los repositorios.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

3. Reinicie la instancia.

```
[ec2-user ~]$ sudo reboot
```

4. Confirme que la versión del kernel se ha actualizado a la versión `4.14.77-70.59` o superior.

```
[ec2-user ~]$ uname -a
```

5. Detenga la instancia y cree una AMI. Para obtener más información, consulte Creación de una AMI basada en Amazon EBS.

CentOS, versión 8 o posterior

Para configurar una AMI de CentOS, versión 8 o posterior, a fin de que sea compatible con la hibernación

1. Actualice el kernel a la versión `4.18.0-305.7.1.el8_4.x86_64` o posterior.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Instale el repositorio Extra Packages for Enterprise Linux (EPEL) de Fedora.

```
[ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

3. Instale el paquete `ec2-hibinit-agent` de los repositorios.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

4. Habilite el agente de hibernación para que se inicie en el arranque.

```
[ec2-user ~]$ sudo systemctl enable hibinit-agent.service
```

5. Reinicie la instancia.

```
[ec2-user ~]$ sudo reboot
```

6. Confirme que la versión del kernel se ha actualizado a la versión `4.18.0-305.7.1.el8_4.x86_64` o posterior.

```
[ec2-user ~]$ uname -a
```

Fedora, versión 34 o posterior

Para configurar una AMI de Fedora, versión 34 o posterior, a fin de que sea compatible con la hibernación

1. Actualice el kernel a la versión `5.12.10-300.fc34.x86_64` o posterior.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Instale el paquete `ec2-hibinit-agent` de los repositorios.

```
[ec2-user ~]$ sudo dnf install ec2-hibinit-agent
```

3. Habilite el agente de hibernación para que se inicie en el arranque.

```
[ec2-user ~]$ sudo systemctl enable hibinit-agent.service
```

4. Reinicie la instancia.

```
[ec2-user ~]$ sudo reboot
```

5. Confirme que la versión del kernel se ha actualizado a la versión `5.12.10-300.fc34.x86_64` o posterior.

```
[ec2-user ~]$ uname -a
```

Red Hat Enterprise Linux, versión 8 o 9

Para configurar una AMI de Red Hat Enterprise Linux 8 o 9 a fin de que sea compatible con la hibernación

1. Actualice el kernel a la versión `4.18.0-305.7.1.el8_4.x86_64` o posterior.

   ```
   [ec2-user ~]$ sudo yum update kernel
   ```

2. Instale el repositorio Extra Packages for Enterprise Linux (EPEL) de Fedora.

   Versión 8 de RHEL:

   ```
   [ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
   ```

   Versión 9 de RHEL:

   ```
   [ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
   ```

3. Instale el paquete `ec2-hibinit-agent` de los repositorios.

   ```
   [ec2-user ~]$ sudo yum install ec2-hibinit-agent
   ```

4. Habilite el agente de hibernación para que se inicie en el arranque.

   ```
   [ec2-user ~]$ sudo systemctl enable hibinit-agent.service
   ```

5. Reinicie la instancia.

   ```
   [ec2-user ~]$ sudo reboot
   ```

6. Confirme que la versión del kernel se ha actualizado a la versión `4.18.0-305.7.1.el8_4.x86_64` o posterior.

```
[ec2-user ~]$ uname -a
```

Ubuntu 20.04 LTS (Focal Fossa) iniciado antes del número de serie 20210820

Para configurar una AMI de Ubuntu 20.04 LTS (Focal Fossa) iniciada antes del número de serie 20210820 con objeto de que sea compatible con la hibernación

1. Actualice el kernel de linux-aws a `5.8.0-1038.40` o posterior y grub2 a `2.04-1ubuntu26.13` o posterior.

   ```
   [ec2-user ~]$ sudo apt update
   [ec2-user ~]$ sudo apt dist-upgrade
   ```

2. Reinicie la instancia.

   ```
   [ec2-user ~]$ sudo reboot
   ```

3. Confirme que la versión del kernel se ha actualizado a la versión `5.8.0-1038.40` o posterior.

   ```
   [ec2-user ~]$ uname -a
   ```

4. Confirme que la versión de grub2 se ha actualizado a la versión `2.04-1ubuntu26.13` o posterior.

   ```
   [ec2-user ~]$ dpkg --list | grep grub2-common
   ```

Ubuntu 18.04 (Bionic Beaver) iniciado con el número de serie 20190722.1

Para configurar una AMI de Ubuntu 18.04 LTS iniciada antes del número de serie 20190722.1 a fin de que sea compatible con la hibernación

1. Actualice el kernel a la versión `4.15.0-1044` o posterior.

   ```
   [ec2-user ~]$ sudo apt update
   [ec2-user ~]$ sudo apt dist-upgrade
   ```

2. Instale el paquete `ec2-hibinit-agent` de los repositorios.

```
[ec2-user ~]$ sudo apt install ec2-hibinit-agent
```

3. Reinicie la instancia.

```
[ec2-user ~]$ sudo reboot
```

4. Confirme que la versión del kernel se ha actualizado a la versión `4.15.0-1044` o posterior.

```
[ec2-user ~]$ uname -a
```

Ubuntu 16.04 (Xenial Xerus)

Para configurar Ubuntu 16.04 LTS a fin de que sea compatible con la hibernación, debe instalar el paquete del kernel linux-aws-hwe, versión 4.15.0-1058-aws o posterior, y ec2-hibinit-agent.

> **Important**
>
> El paquete del kernel `linux-aws-hwe` es compatible con Canonical. El soporte estándar para Ubuntu 16.04 LTS finalizó en abril de 2021 y el paquete ya no recibe actualizaciones periódicas. Sin embargo, recibirá actualizaciones de seguridad adicionales hasta que finalice el soporte de mantenimiento de seguridad extendido en 2024. Para obtener más información, consulte Amazon EC2 Hibernation for Ubuntu 16.04 LTS now available en el blog de Canonical Ubuntu.
> Le recomendamos que actualice a la AMI de Ubuntu 20.04 LTS (Focal Fossa) o la AMI de Ubuntu 18.04 LTS (Bionic Beaver).

Para configurar una AMI Ubuntu 16.04 LTS para que admita la hibernación

1. Actualice el kernel a la versión `4.15.0-1058-aws` o posterior.

```
[ec2-user ~]$ sudo apt update
[ec2-user ~]$ sudo apt install linux-aws-hwe
```

2. Instale el paquete `ec2-hibinit-agent` de los repositorios.

```
[ec2-user ~]$ sudo apt install ec2-hibinit-agent
```

3. Reinicie la instancia.

```
[ec2-user ~]$ sudo reboot
```

4. Confirme que la versión del kernel se ha actualizado a la versión `4.15.0-1058-aws` o posterior.

```
[ec2-user ~]$ uname -a
```

Habilitación de la hibernación para una instancia de Amazon EC2

A fin de hibernar una instancia, primero debe habilitarla para la hibernación al iniciar la instancia.

> **Important**
>
> No puede habilitar o deshabilitar la hibernación para una instancia después de iniciarla.

Temas

- Habilitación de la hibernación de instancias bajo demanda
- Habilitación de la hibernación de instancias de spot
- Comprobación de si una instancia está habilitada para la hibernación

Habilitación de la hibernación de instancias bajo demanda

Utilice uno de los siguientes métodos para habilitar la hibernación de las instancias bajo demanda.

New console

Habilitación de la hibernación de una instancia bajo demanda

1. Siga el procedimiento para iniciar una instancia, pero no la lance hasta que haya completado los siguientes pasos para habilitar la hibernación.
2. Para habilitar la hibernación, configure los siguientes campos en el asistente de inicialización de instancias:

a. En Application and OS Images (Imagen de máquina de Amazon) (Imágenes de aplicaciones y sistema operativo [Imagen de máquina de Amazon]), seleccione una AMI que admita la hibernación. Para obtener más información, consulte AMI.

b. En Tipo de instancia, elija un tipo de instancia admitido. Para obtener más información, consulte Familias de instancias.

c. En Configure storage (Configurar almacenamiento), elija Advanced (Avanzado) a la derecha y especifique la siguiente información para el volumen raíz:

- En Tamaño (GiB), especifique el tamaño del volumen raíz de EBS. El volumen debe ser lo suficientemente grande como para almacenar el contenido de la RAM y adaptarse al uso esperado.
- En Volume Type (Tipo de volumen), seleccione un tipo de volumen de EBS admitido: SSD de uso general (`gp2` y `gp3`) o SSD de IOPS aprovisionadas (`io1` y `io2`).
- En Encrypted (Cifrado), elija Yes (Sí). Si habilitó el cifrado de forma predeterminada en esta región de AWS, la opción Yes (Sí) estará seleccionada.
- En KMS key (Clave de KMS), seleccione la clave de cifrado del volumen. Si ha habilitado el cifrado de forma predeterminada en esta región de AWS, se selecciona la clave de cifrado predeterminada.

Para obtener más información acerca de los requisitos previos del volumen raíz, consulte Requisitos previos para la hibernación de instancias de Amazon EC2.

d. Expanda Advanced details (Detalles avanzados) y, para Stop - Hibernate behavior (Detener: comportamiento de hibernación), elija Enable (Habilitar).

3. En el panel Summary (Resumen), revise la configuración de la instancia y, a continuación, elija Launch instance (iniciar instancia). Para obtener más información, consulte Lance una instancia con el nuevo asistente de inicialización de instancias.

Old console

Habilitación de la hibernación de una instancia bajo demanda

1. Siga el procedimiento indicado en Lance una instancia con el antiguo asistente de inicialización de instancias.

2. En la página Elegir una Amazon Machine Image (AMI), seleccione una AMI que admita la hibernación. Para obtener más información acerca de las AMI, consulte Requisitos previos para la hibernación de instancias de Amazon EC2.
3. En la página Choose an Instance Type (Elegir un tipo de instancia), seleccione un tipo de instancia compatible y elija Next: Configure Instance Details (Siguiente: Configurar detalles de instancia). Para obtener información acerca de los tipos de instancia admitidos, consulte Requisitos previos para la hibernación de instancias de Amazon EC2.
4. En la página Configure Instance Details (Configurar detalles de instancia), para Stop - Hibernate Behavior (Detener: Comportamiento de hibernación), active la casilla Enable hibernation as an additional stop behavior (Habilitar la hibernación como un comportamiento de detención adicional).
5. En la página Adición de almacenamiento, para el volumen raíz, especifique la siguiente información:

   - En Size (GiB) (Tamaño [GiB]), especifique el tamaño del volumen raíz de EBS. El volumen debe ser lo suficientemente grande como para almacenar el contenido de la RAM y adaptarse al uso esperado.
   - En Volume Type (Tipo de volumen), seleccione un tipo de volumen de EBS compatible, SSD de uso general (`gp2` y `gp3`) o SSD de IOPS provisionadas (`io1` y `io2`).
   - En Cifrado, seleccione la clave de cifrado del volumen. Si ha habilitado el cifrado de forma predeterminada en esta región de AWS, se selecciona la clave de cifrado predeterminada.

   Para obtener más información acerca de los requisitos previos del volumen raíz, consulte Requisitos previos para la hibernación de instancias de Amazon EC2.
6. Continúe tal y como se lo indique el asistente. Cuando haya acabado de revisar las opciones de la página Review Instance Launch (Revisar inicialización de instancia), elija Launch (iniciar). Para obtener más información, consulte Lance una instancia con el antiguo asistente de inicialización de instancias.

AWS CLI

Habilitación de la hibernación de una instancia bajo demanda

Utilice el comando run-instances para iniciar una instancia. Especifique los parámetros del volumen raíz de EBS mediante el parámetro `--block-device-mappings file://`

`mapping.json` y habilite la hibernación mediante el parámetro `--hibernation-options Configured=true`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type m5.large \
    --block-device-mappings file://mapping.json \
    --hibernation-options Configured=true \
    --count 1 \
    --key-name MyKeyPair
```

En `mapping.json`, especifique lo siguiente.

```
[
    {
        "DeviceName": "/dev/xvda",
        "Ebs": {
            "VolumeSize": 30,
            "VolumeType": "gp2",
            "Encrypted": true
        }
    }
]
```

> **Note**
>
> El valor de `DeviceName` debe coincidir con el nombre del dispositivo raíz que está asociado a la AMI. Para buscar el nombre del dispositivo raíz, utilice el comando describe-images.
>
> ```
> aws ec2 describe-images --image-id ami-0abcdef1234567890
> ```
>
> Si ha habilitado el cifrado de forma predeterminada en esta región de AWS, puede omitir `"Encrypted": true`.

PowerShell

Habilitación la hibernación de una instancia bajo demanda con AWS Tools for Windows PowerShell

Utilice el comando New-EC2Instance para iniciar una instancia. Especifique el volumen raíz de EBS definiendo primero la asignación de dispositivos de bloque y, a continuación, agregándola al comando mediante el parámetro `-BlockDeviceMappings`. Habilite la hibernación con el parámetro `-HibernationOptions_Configured $true`.

```
PS C:\> $ebs_encrypt = New-Object Amazon.EC2.Model.BlockDeviceMapping
PS C:\> $ebs_encrypt.DeviceName = "/dev/xvda"
PS C:\> $ebs_encrypt.Ebs = New-Object Amazon.EC2.Model.EbsBlockDevice
PS C:\> $ebs_encrypt.Ebs.VolumeSize = 30
PS C:\> $ebs_encrypt.Ebs.VolumeType = "gp2"
PS C:\> $ebs_encrypt.Ebs.Encrypted = $true

PS C:\> New-EC2Instance `
              -ImageId ami-0abcdef1234567890 `
              -InstanceType m5.large `
              -BlockDeviceMappings $ebs_encrypt `
              -HibernationOptions_Configured $true `
              -MinCount 1 `
              -MaxCount 1 `
              -KeyName MyKeyPair
```

> **Note**
>
> El valor de `DeviceName` debe coincidir con el nombre del dispositivo raíz asociado a la AMI. Para buscar el nombre del dispositivo raíz, utilice el comando Get-EC2Image.
>
> ```
> Get-EC2Image -ImageId ami-0abcdef1234567890
> ```
>
> Si ha habilitado el cifrado de forma predeterminada en esta región de AWS, puede omitir `Encrypted = $true` de la asignación de dispositivos de bloque.

Habilitación de la hibernación de instancias de spot

Utilice uno de los siguientes métodos para habilitar la hibernación de las instancias de spot. Para obtener más información sobre la hibernación de una instancia de spot interrumpida, consulte Interrupciones de instancias de spot.

Console

Puede utilizar el asistente de inicialización de instancias en la consola de Amazon EC2 para habilitar la hibernación de una instancia de spot.

Habilitación de la hibernación de una instancia de spot

1. Siga el procedimiento para solicitar una instancia de spot con el asistente de inicialización de instancias, pero no la lance hasta que haya completado los siguientes pasos para habilitar la hibernación.
2. Para habilitar la hibernación, configure los siguientes campos en el asistente de inicialización de instancias:

   a. En Application and OS Images (Imagen de máquina de Amazon) (Imágenes de aplicaciones y sistema operativo [Imagen de máquina de Amazon]), seleccione una AMI que admita la hibernación. Para obtener más información, consulte AMI.

   b. En Tipo de instancia, elija un tipo de instancia admitido. Para obtener más información, consulte Familias de instancias.

   c. En Configure storage (Configurar almacenamiento), elija Advanced (Avanzado) a la derecha y especifique la siguiente información para el volumen raíz:

      - En Tamaño (GiB), especifique el tamaño del volumen raíz de EBS. El volumen debe ser lo suficientemente grande como para almacenar el contenido de la RAM y adaptarse al uso esperado.
      - En Volume Type (Tipo de volumen), seleccione un tipo de volumen de EBS admitido: SSD de uso general (`gp2` y `gp3`) o SSD de IOPS aprovisionadas (`io1` y `io2`).
      - En Encrypted (Cifrado), elija Yes (Sí). Si habilitó el cifrado de forma predeterminada en esta región de AWS, la opción Yes (Sí) estará seleccionada.
      - En KMS key (Clave de KMS), seleccione la clave de cifrado del volumen. Si ha habilitado el cifrado de forma predeterminada en esta región de AWS, se selecciona la clave de cifrado predeterminada.

      Para obtener más información acerca de los requisitos previos del volumen raíz, consulte Requisitos previos para la hibernación de instancias de Amazon EC2.

   d. Amplíe Detalles avanzados y, además de los campos para configurar una instancia de spot, haga lo siguiente:

i. En Tipo de solicitud, elija Persistente.

ii. En Comportamiento de interrupción, seleccione Hibernar. Como alternativa, en Detener: comportamiento de hibernación, seleccione Habilitar. Ambos campos habilitan la hibernación en su instancia de spot. Solo necesita configurar uno de ellos.

3. En el panel Summary (Resumen), revise la configuración de la instancia y, a continuación, elija Launch instance (iniciar instancia). Para obtener más información, consulte Lance una instancia con el nuevo asistente de inicialización de instancias.

AWS CLI

Puede habilitar la hibernación de una instancia de spot mediante el comando de la AWS CLI run-instances.

Habilitación de la hibernación de una instancia de spot con el parámetro **`hibernation-options`**

Utilice el comando run-instances para solicitar una instancia de spot. Especifique los parámetros del volumen raíz de EBS mediante el parámetro `--block-device-mappings file://mapping.json` y habilite la hibernación mediante el parámetro `--hibernation-options Configured=true`. El tipo de solicitud de spot (`SpotInstanceType`) debe ser `persistent`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c4.xlarge \
    --block-device-mappings file://mapping.json \
    --hibernation-options Configured=true \
    --count 1 \
    --key-name MyKeyPair
    --instance-market-options
        {
           "MarketType":"spot",
           "SpotOptions":{
              "MaxPrice":"1",
              "SpotInstanceType":"persistent"
            }
        }
```

Especifique los parámetros del volumen raíz de EBS en `mapping.json` de la siguiente manera.

```
[
    {
        "DeviceName": "/dev/xvda",
        "Ebs": {
            "VolumeSize": 30,
            "VolumeType": "gp2",
            "Encrypted": true
        }
    }
]
```

> **Note**
>
> El valor de `DeviceName` debe coincidir con el nombre del dispositivo raíz que está asociado a la AMI. Para buscar el nombre del dispositivo raíz, utilice el comando describe-images.
>
> ```
> aws ec2 describe-images --image-id ami-0abcdef1234567890
> ```
>
> Si ha habilitado el cifrado de forma predeterminada en esta región de AWS, puede omitir `"Encrypted": true`.

PowerShell

Para habilitar la hibernación de una instancia de spot con AWS Tools for Windows PowerShell

Utilice el comando New-EC2Instance para solicitar una instancia de spot. Especifique el volumen raíz de EBS definiendo primero la asignación de dispositivos de bloque y, a continuación, agregándola al comando mediante el parámetro `-BlockDeviceMappings`. Habilite la hibernación con el parámetro `-HibernationOptions_Configured $true`.

```
PS C:\> $ebs_encrypt = New-Object Amazon.EC2.Model.BlockDeviceMapping
PS C:\> $ebs_encrypt.DeviceName = "/dev/xvda"
PS C:\> $ebs_encrypt.Ebs = New-Object Amazon.EC2.Model.EbsBlockDevice
PS C:\> $ebs_encrypt.Ebs.VolumeSize = 30
PS C:\> $ebs_encrypt.Ebs.VolumeType = "gp2"
PS C:\> $ebs_encrypt.Ebs.Encrypted = $true

PS C:\> New-EC2Instance `
```

```
            -ImageId ami-0abcdef1234567890 `
            -InstanceType m5.large `
            -BlockDeviceMappings $ebs_encrypt `
            -HibernationOptions_Configured $true `
            -MinCount 1 `
            -MaxCount 1 `
            -KeyName MyKeyPair `
            -InstanceMarketOption @(
                  MarketType = spot;
                  SpotOptions @{
                  MaxPrice = 1;
                  SpotInstanceType = persistent}
               )
```

> **Note**
>
> El valor de `DeviceName` debe coincidir con el nombre del dispositivo raíz asociado a la AMI. Para buscar el nombre del dispositivo raíz, utilice el comando Get-EC2Image.
>
> ```
> Get-EC2Image -ImageId ami-0abcdef1234567890
> ```
>
> Si ha habilitado el cifrado de forma predeterminada en esta región de AWS, puede omitir `Encrypted = $true` de la asignación de dispositivos de bloque.

Hay varias formas de habilitar la hibernación de una instancia de spot. Para obtener más información, consulte Especificar el comportamiento de interrupción.

Comprobación de si una instancia está habilitada para la hibernación

Utilice las siguientes instrucciones para ver si una instancia está habilitada para la hibernación.

Console

Comprobación de si la instancia está habilitada para la hibernación

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Seleccione la instancia y en la pestaña Details (Detalles), en la sección Instance details (Detalles de instancia), inspeccione Stop-hibernate behavior (Comportamiento de detención

de hibernación). Enabled (Habilitado) indica que la instancia está habilitada para la hibernación.

AWS CLI

Comprobación de si la instancia está habilitada para la hibernación

Utilice el comando describe-instances y especifique el parámetro `--filters "Name=hibernation-options.configured,Values=true"` para filtrar instancias que están habilitadas para la hibernación.

```
aws ec2 describe-instances \
    --filters "Name=hibernation-options.configured,Values=true"
```

El siguiente campo del resultado indica que la instancia está habilitada para la hibernación.

```
"HibernationOptions": {
    "Configured": true
}
```

PowerShell

Para ver si la instancia está habilitada para la hibernación utilizando la AWS Tools for Windows PowerShell

Utilice el comando Get-EC2Instance y especifique el parámetro `-Filter @{ Name="hibernation-options.configured"; Value="true"}` para filtrar instancias que están habilitadas para la hibernación.

```
(Get-EC2Instance -Filter @{Name="hibernation-options.configured";
 Value="true"}).Instances
```

La salida enumera las instancias de EC2 que están habilitadas para la hibernación.

Deshabilitación de KASLR en una instancia (solo Ubuntu)

Para ejecutar la hibernación en una instancia recién iniciada con Ubuntu 16.04 LTS (Xenial Xerus), Ubuntu 18.04 LTS (Bionic Beaver) iniciada con el número de serie 20190722.1 o posterior,

o Ubuntu 20.04 LTS (Focal Fossa) iniciada con el número de serie 20210820 o posterior, le recomendamos que deshabilite KASLR (Kernel Address Space Layout Randomization). En Ubuntu 16.04 LTS, Ubuntu 18.04 LTS o Ubuntu 20.04 LTS, KASLR está habilitado de forma predeterminada.

KASLR es una característica de seguridad de kernel de Linux estándar que contribuye a mitigar la exposición y ramificaciones de vulnerabilidades de acceso a memoria aún no detectadas aleatorizando el valor de dirección base del kernel. Con KASLR habilitado, existe la posibilidad de que la instancia no se pueda reanudar si se ha hibernado.

Para obtener más información sobre KASLR, consulte Características de Ubuntu.

Para deshabilitar KASLR en una instancia iniciada con Ubuntu

1. Conéctese a la instancia mediante SSH. Para obtener más información, consulte the section called “Conéctese con SSH desde macOS o Linux”.
2. Abra el archivo `/etc/default/grub.d/50-cloudimg-settings.cfg` con el editor que prefiera. Edite la línea `GRUB_CMDLINE_LINUX_DEFAULT` para adjuntar la opción `nokaslr` a su extremo, tal como se muestra en el ejemplo siguiente.

   ```
   GRUB_CMDLINE_LINUX_DEFAULT="console=tty1 console=ttyS0
    nvme_core.io_timeout=4294967295 nokaslr"
   ```
3. Guarde el archivo y salga del editor.
4. Ejecute el siguiente comando para volver a compilar la configuración de grub.

   ```
   [ec2-user ~]$ sudo update-grub
   ```
5. Reinicie la instancia.

   ```
   [ec2-user ~]$ sudo reboot
   ```
6. Ejecute el siguiente comando para confirmar que `nokaslr` se ha agregado.

   ```
   [ec2-user ~]$ cat /proc/cmdline
   ```

   La salida del comando debería incluir la opción `nokaslr`.

Hibernación de una instancia de Amazon EC2

Puede iniciar la hibernación en una instancia bajo demanda o en una instancia de spot si la instancia es una instancia respaldada por EBS, está habilitada para la hibernación y cumple los requisitos previos de hibernación. Si una instancia no se puede hibernar correctamente, se produce un apagado normal.

Console

Habilitación de una instancia

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancias).
3. Seleccione una instancia y elija Instance State (Estado de la instancia) y después Hibernate instance (Hibernar instancia). Si la opción Hibernate instance (Hibernar instancia) está desactivada, la instancia ya está hibernada o detenida, o no se puede hibernar. Para obtener más información, consulte Requisitos previos para la hibernación de instancias de Amazon EC2.
4. Cuando le pidan confirmación, elija Hibernate (Hibernar). Puede que transcurran unos minutos hasta que la instancia se hiberne. El estado de la instancia primero cambia a Stopping (Deteniéndose) y, luego, cambia a Stopped (Detenida) cuando la instancia ha hibernado.

AWS CLI

Habilitación de una instancia respaldada por EBS

Use el comando stop-instances y especifique el parámetro `--hibernate`.

```
aws ec2 stop-instances \
    --instance-ids i-1234567890abcdef0 \
    --hibernate
```

PowerShell

Habilitación de una instancia con AWS Tools for Windows PowerShell

Use el comando Stop-EC2Instance y especifique el parámetro `-Hibernate $true`.

```
Stop-EC2Instance `
    -InstanceId i-1234567890abcdef0 `
    -Hibernate $true
```

Console

Comprobación de si la hibernación se inició en una instancia

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Seleccione la instancia y, en la pestaña Detalles, en la sección Detalles de la instancia, compruebe el valor de Mensaje de transición de estado.

   El mensaje Client.UserInitiatedHibernate: hibernación iniciada por el usuario indica que inició la hibernación en la instancia bajo demanda o en la instancia de spot.

AWS CLI

Comprobación de si la hibernación se inició en una instancia

Utilice el comando describe-instances y especifique el filtro `state-reason-code` para ver instancias en las que se ha iniciado la hibernación.

```
aws ec2 describe-instances \
    --filters "Name=state-reason-code,Values=Client.UserInitiatedHibernate"
```

El siguiente campo de la salida indica que la hibernación se inició en la instancia bajo demanda o en la instancia de spot.

```
"StateReason": {
    "Code": "Client.UserInitiatedHibernate"
}
```

PowerShell

Para ver si la hibernación se inició en una instancia utilizando la AWS Tools for Windows PowerShell

Utilice el comando Get-EC2Instance y especifique el filtro `state-reason-code` para ver instancias en las que se ha iniciado la hibernación.

```
Get-EC2Instance `
    -Filter @{Name="state-reason-code";Value="Client.UserInitiatedHibernate"}
```

La salida enumera las instancias de EC2 en las que se ha iniciado la hibernación.

Inicio de una instancia hibernada de Amazon EC2

Inicie una instancia hibernada iniciándola de la misma forma que iniciaría una instancia detenida.

> **Note**
>
> En el caso de las instancias de spot, si Amazon EC2 ha puesto en hibernación la instancia, solo Amazon EC2 podrá reanudarla. Solo puede reanudar una instancia de spot en hibernación si usted la ha puesto en dicho estado. Las instancias de spot solo se pueden reanudar si hay capacidad disponible y el precio de spot es menor o igual que el precio máximo especificado.

Console

Reinicio de una instancia hibernada

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancias).
3. Seleccione una instancia que esté en hibernación y elija Instance State (Estado de la instancia) y Start instance (Iniciar instancia). Puede que transcurran unos minutos hasta que la instancia pase al estado `running`. Durante este tiempo, las comprobaciones de estado de la instancia muestran la instancia en un estado erróneo hasta que esta se inicie.

AWS CLI

Reinicio de una instancia hibernada

Utilice el comando start-instances.

```
aws ec2 start-instances \
```

```
    --instance-ids i-1234567890abcdef0
```

PowerShell

Para iniciar una instancia hibernada utilizando la AWS Tools for Windows PowerShell

Utilice el comando Start-EC2Instance.

```
Start-EC2Instance `
    -InstanceId i-1234567890abcdef0
```

Solución de problemas de hibernación de la instancia de Amazon EC2

Utilice esta información como ayuda para diagnosticar y solucionar problemas que pueda encontrar al hibernar una instancia.

Problemas de hibernación

- No se puede hibernar de inmediato después de un inicialización
- La transición tarda demasiado de stopping a stopped, y el estado de la memoria no se reinicia después del inicio
- instancia “bloqueada” en el estado de detención
- No se puede iniciar la instancia de spot inmediatamente después de la hibernación
- Error al reanudar instancias de spot

No se puede hibernar de inmediato después de un inicialización

Si intenta hibernar una instancia demasiado rápido después de haberla iniciado, recibirá un error.

Debe esperar al menos dos minutos para las instancias de Linux y unos cinco minutos para las de Windows después de la inicialización para poder hibernar.

La transición tarda demasiado de **`stopping`** a **`stopped`**, y el estado de la memoria no se reinicia después del inicio

Si su instancia de hibernación tarda mucho en realizar la transición del estado `stopping` a `stopped` y si el estado de la memoria no se restablece después del inicio, esto podría indicar que la hibernación no se configuró correctamente.

instancias de Linux

Compruebe el registro del sistema de la instancia y busque mensajes que estén relacionados con la hibernación. Para obtener acceso al registro del sistema, conéctese a la instancia o utilice el comando get-console-output. Busque líneas de registro desde `hibinit-agent`. Si las líneas de registro indican un error o faltan, es probable que se haya producido un error al configurar la hibernación en el momento de la inicialización.

Por ejemplo, el siguiente mensaje indica que el volumen raíz de la instancia no es lo suficientemente grande: `hibinit-agent: Insufficient disk space. Cannot create setup for hibernation. Please allocate a larger root device.`

Si la última línea de registro de `hibinit-agent` es `hibinit-agent: Running: swapoff /swap`, la hibernación se ha configurado correctamente.

Si no ve los registros de estos procesos, es posible que su AMI no admita la hibernación. Para obtener información acerca de las AMI soportadas, consulte Requisitos previos para la hibernación de instancias de Amazon EC2. Si utilizó su propia AMI de Linux, asegúrese de que haya seguido las instrucciones para Configuración de una AMI de Linux para que admita la hibernación.

Windows Server 2016 y versiones posteriores

Compruebe el registro de la inicialización de EC2 y busque mensajes que estén relacionados con la hibernación. Para acceder al registro de la inicialización de EC2, conéctese a la instancia y abra el archivo `C:\ProgramData\Amazon\EC2-Windows\Launch\Log\Ec2Launch.log` en un editor de texto. Si utiliza EC2Launch v2, abra `C:\ProgramData\Amazon\EC2Launch\log\agent.log`.

> **Note**
>
> De manera predeterminada, Windows oculta los archivos y las carpetas en `C:\ProgramData`. Para ver los directorios y los archivos de inicialización de EC2, escriba la ruta de acceso en Windows Explorer o cambie las propiedades de carpeta para ver los archivos y carpetas ocultos.

Busque las líneas de registro de la hibernación. Si las líneas de registro indican un error o faltan, es probable que se haya producido un error al configurar la hibernación en el momento de la inicialización.

Por ejemplo, el siguiente mensaje indica que no se pudo configurar la hibernación: `Message: Failed to enable hibernation.` Si el mensaje de error incluye valores ASCII decimales, puede convertirlos en texto sin formato para leer el mensaje completo.

Si la línea de registro contiene `HibernationEnabled: true`, la hibernación se ha configurado correctamente.

Windows Server 2012 R2 y versiones anteriores

Compruebe el registro de configuración de EC2 y busque mensajes que estén relacionados con la hibernación. Para acceder al registro de configuración de EC2, conéctese a la instancia y abra el archivo `C:\Program Files\Amazon\Ec2ConfigService\Logs\Ec2ConfigLog.txt` en un editor de texto. Busque líneas de registro para `SetHibernateOnSleep`. Si las líneas de registro indican un error o faltan, es probable que se haya producido un error al configurar la hibernación en el momento de la inicialización.

Por ejemplo, el siguiente mensaje indica que el volumen raíz de la instancia no es lo suficientemente grande: `SetHibernateOnSleep: Failed to enable hibernation: Hibernation failed with the following error: There is not enough space on the disk.`

Si la línea de registro es `SetHibernateOnSleep: HibernationEnabled: true`, la hibernación se ha configurado correctamente.

Tamaño de las instancias de Windows

Si utiliza una instancia T3 o T3a de Windows con menos de 1 GB de RAM, intente aumentar el tamaño de la instancia a una que tenga al menos 1 GB de RAM.

instancia “bloqueada” en el estado de detención

Si hibernó su instancia y aparece bloqueada en el estado `stopping`, puede forzar la detención. Para obtener más información, consulte Solucionar problemas de detención de la instancia.

No se puede iniciar la instancia de spot inmediatamente después de la hibernación

Si intenta iniciar una instancia de spot en los dos minutos siguientes a su hibernación, es posible que aparezca el siguiente error:

```
You failed to start the Spot Instance because the associated Spot Instance request is not in an appropriate state to support start.
```

Espere unos dos minutos para las instancias de Linux y unos cinco minutos para las de Windows y, a continuación, vuelva a intentar iniciar la instancia.

Error al reanudar instancias de spot

Si su instancia de spot se hibernó correctamente pero no se pudo reanudar y, en cambio, se reinició (un reinicio nuevo en el que no se conserva el estado de hibernación), es posible que los datos del usuario contengan el siguiente script:

```
/usr/bin/enable-ec2-spot-hibernation
```

Elimine este script del campo Datos de usuario de la plantilla de inicialización y, a continuación, solicite una nueva instancia de spot.

Tenga en cuenta que, aunque la instancia no se pueda reanudar, si no se conserva el estado de hibernación, la instancia se puede iniciar de la misma manera que si se iniciara desde el estado `stopped`.

Reinicio de su instancia

Un reinicio de instancia es equivalente a un reinicio del sistema operativo. En la mayoría de los casos, solo necesita unos minutos para reiniciar su instancia.

Cuando reinicia una instancia, conserva lo siguiente:

- Nombre de DNS público (IPv4)
- Dirección IPv4 privada
- Dirección IPv4 pública
- Dirección IPv6 (si corresponde)
- Cualquier dato de los volúmenes de su almacén de instancias

Con el reinicio de una instancia, no se comienza un período nuevo de facturación de instancia (con un cargo mínimo de un minuto), a diferencia de detener e iniciar la instancia.

La instancia se puede programar para que se reinicie durante las tareas de mantenimiento necesarias, tales como la instalación de actualizaciones que requieren reinicio. No se requiere ninguna acción por su parte; le recomendamos que espere a que se produzca el reinicio dentro del periodo programado. Para obtener más información, consulte Eventos programados para las instancias.

Le recomendamos que utilice la consola de Amazon EC2, una herramienta de la línea de comandos o la API de Amazon EC2 para reiniciar la instancia en lugar de ejecutar el comando de reinicio del

sistema operativo desde la instancia. Si utiliza la consola de Amazon EC2, una herramienta de la línea de comandos o la API de Amazon EC2 para reiniciar la instancia, se lleva a cabo un reinicio en frío si la instancia no se cierra limpiamente al cabo de cuatro minutos. Si utiliza AWS CloudTrail, al utilizar Amazon EC2 para reiniciar la instancia, también se crea un registro de API del momento en que se reinició su instancia.

instancias de Windows

Si Windows está instalando actualizaciones en la instancia, le recomendamos que no reinicie ni apague la instancia con la consola de Amazon EC2 ni con la línea de comando hasta que se hayan instalado todas las actualizaciones. Cuando se usa la consola de Amazon EC2 o la línea de comando para reiniciar o apagar una instancia, existe el riesgo de que se lleve a cabo un reinicio en frío de la instancia. Un reinicio en frío mientras se están instalando actualizaciones podría dejar la instancia en un estado inestable.

Console

Para reiniciar una instancia con la console

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Seleccione la instancia y elija Instance state (Estado de instancia) y Reboot instance (Reiniciar instancia).

   Alternativamente, seleccione la instancia y elija Actions (Acciones), Manage instance state (Administrar el estado de la instancia). En la pantalla que se abre, elija Reboot (Reiniciar) y, luego, Change state (Cambiar estado).
4. Cuando se le indique que confirme, elija Reboot (Reiniciar).

   La instancia permanece en el estado de `running`.

Command line

Reinicio de una instancia

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

- reboot-instances (AWS CLI)

- Restart-EC2Instance (AWS Tools for Windows PowerShell)

Para ejecutar un experimento controlado de inserción de errores

Puede usar AWS Fault Injection Service para probar cómo responde la aplicación cuando la instancia se reinicia. Para obtener más información, consulte la Guía del usuario de AWS Fault Injection Service.

Terminación de las instancias de Amazon EC2

Puede eliminar la instancia cuando ya no la necesite. Esto se denomina terminar la instancia. En cuanto el estado de una instancia cambia a `shutting-down` o `terminated`, dejará de incurrir en gastos por ella.

Una vez se ha terminado la instancia, no es posible conectarse a ella ni iniciarla. No obstante, puede iniciar instancias adicionales utilizando la misma AMI. Si prefiere detener o poner a hibernar una instancia, consulte Detención e iniciación de una instancia de Amazon EC2 o Hibernación de la instancia de Amazon EC2. Para obtener más información, consulte Diferencias entre reinicio, detención, hibernación y terminación.

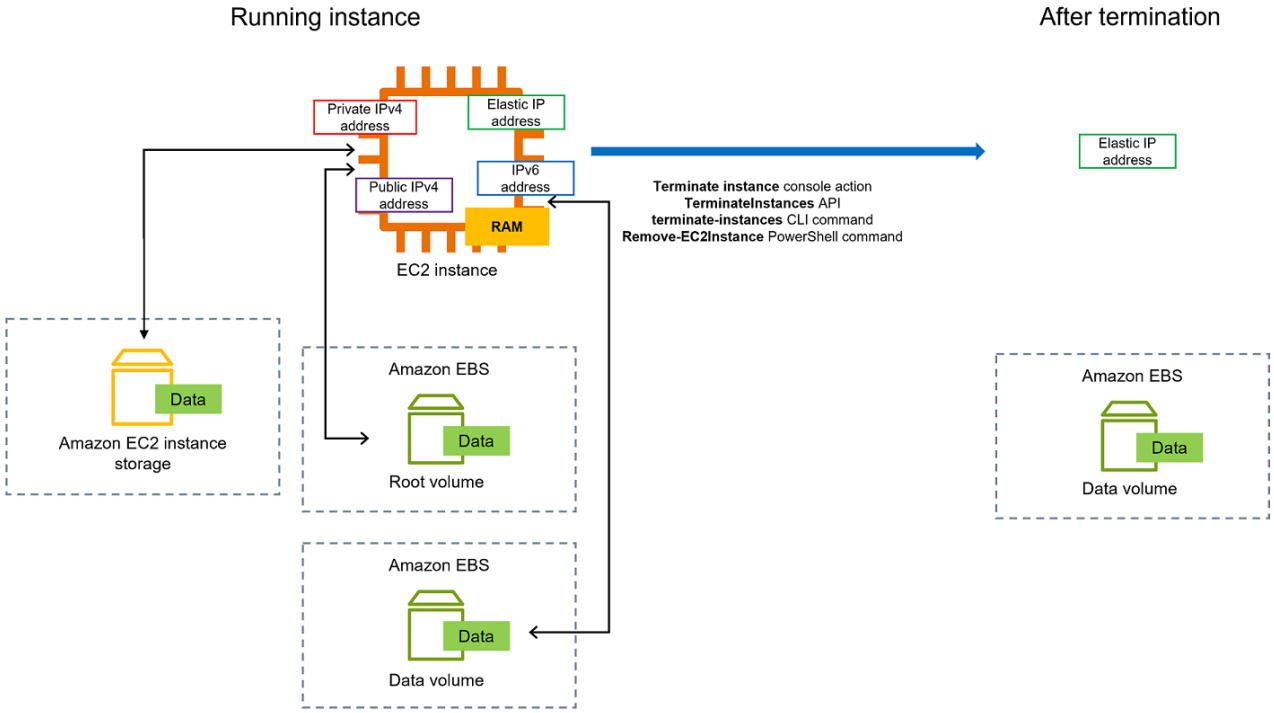
Contenido

Cómo funciona la terminación de instancias

Cuando se termina una instancia, los cambios se registran en el nivel del SO de la instancia, algunos recursos se pierden y otros persisten.

En el siguiente diagrama se muestra lo que se pierde y lo que persiste cuando se termina una instancia de Amazon EC2. Cuando una instancia termina, los datos de cualquier volumen de almacén de instancias y los datos almacenados en la RAM de instancias se borran. Cualquier

dirección IP elástica asociada a la instancia se desvincula. En el caso de los volúmenes de Amazon EBS y los datos de esos volúmenes, el resultado depende de la configuración Eliminar al terminar del volumen. De manera predeterminada, el volumen raíz se elimina y los volúmenes de datos se conservan.



Consideraciones

- Cuando una instancia se termina, los datos de cualquier volumen de almacén de instancias asociado con ella se eliminan.
- De forma predeterminada, los volúmenes de dispositivo raíz de Amazon EBS se eliminan automáticamente cuando se termina la instancia. Sin embargo, los volúmenes de EBS adicionales que asocie en la inicialización o cualquier volumen de EBS que asocie a una instancia existente se mantienen incluso después de que la instancia se termine. Para obtener más información, consulte Conservación de los datos cuando se termina una instancia.

> **Note**
>
> Los volúmenes que no se eliminen tras la terminación de la instancia seguirán incurriendo en cargos.

- Para evitar que alguien termine una instancia accidentalmente, active la protección de terminación.

- Para controlar si una instancia se detiene o termina cuando comienza el cierre desde la instancia, cambie el comportamiento del cierre iniciado por la instancia.
- Si ejecuta un script en la terminación de la instancia, podría producirse una terminación anormal porque no hay forma de asegurarse de que se ejecuten los scripts de apagado. Amazon EC2 intenta apagar una instancia de forma limpia y ejecutar los scripts de apagado del sistema; sin embargo, algunos eventos (como error de hardware) pueden impedir que se ejecuten estos scripts de apagado del sistema.

Qué ocurre cuando se termina una instancia

Cambios registrados a nivel de SO

- La solicitud de la API envía un evento de pulsación de botón al invitado.
- Hay varios servicios del sistema que se detienen como resultado del evento de pulsación del botón. El apagado correcto del sistema lo proporcionan systemd (Linux) o el proceso del sistema (Windows). El apagado estable se activa desde el hipervisor a través del evento de pulsación del botón de apagado de ACPI.
- Se inicia el apagado de ACPI.
- La instancia se apaga cuando se termina el proceso de apagado estable. El tiempo de apagado del SO no puede configurarse. La instancia permanecerá visible en la consola durante un breve periodo y, a continuación, la entrada se eliminará automáticamente.

Recursos perdidos

- Los datos almacenados en los volúmenes del almacén de instancias.
- Los datos almacenados en los volúmenes de los dispositivos raíz de Amazon EBS si el atributo `DeleteOnTermination` está establecido en true.

Recursos que persisten

- Los datos almacenados en volúmenes adicionales de Amazon EBS asociados en la inicialización o después de la inicialización de una instancia.

Respuesta de la aplicación de prueba a la terminación de la instancia

Puede usar AWS Fault Injection Service para probar cómo responde la aplicación cuando la instancia se termina. Para obtener más información, consulte la Guía del usuario de AWS Fault Injection Service.

Finalizar una instancia

Puede terminar una instancia en cualquier momento.

Console

Para terminar una instancia mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancias).
3. Seleccione la instancia y elija Instance state (Estado de la instancia) y Terminate instance (Terminar instancia).
4. Cuando se le indique que confirme, elija Terminar.
5. Tras terminar una instancia, ésta permanece visible durante un breve periodo de tiempo, con un estado `terminated`.

   Si se produce un error en la terminación o si una instancia terminada permanece visible durante más de unas horas, consulte Las instancias que han terminado se siguen mostrando.

Command line

Para terminar una instancia 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 Acceder a Amazon EC2.

- terminate-instances (AWS CLI)
- Remove-EC2Instance (AWS Tools for Windows PowerShell)

Solucionar problemas de terminación de instancias

El solicitante debe tener permiso para llamar a `ec2:TerminateInstances`. Para obtener más información, consulte Ejemplos de políticas para trabajar con instancias.

Si termina la instancia y comienza otra instancia, lo más probable es que haya configurado el escalado automático a través de una característica como flota de EC2 o Amazon EC2 Auto Scaling. Para obtener más información, consulte Instancias lanzadas o terminadas automáticamente.

No se puede finalizar una instancia si está activada la protección contra cancelación. Para obtener más información, consulte protección contra cancelación.

Si la instancia se encuentra en estado `shutting-down` durante más tiempo del habitual, se limpiará (terminará) por procesos automáticos dentro del servicio de Amazon EC2. Para obtener más información, consulte Retrasar la terminación de una instancia.

Cómo habilitar la protección contra la terminación

Si quiere evitar que la instancia se termine accidentalmente, puede habilitar la protección contra terminación para la instancia. El atributo `DisableApiTermination` controla si la instancia puede terminarse mediante la AWS Management Console, la AWS Command Line Interface (AWS CLI) o la API. De forma predeterminada, la protección contra terminación está deshabilitada para la instancia, lo que significa que la instancia se puede cerrar mediante la AWS Management Console, la AWS CLI o la API. Puede establecer el valor de este atributo cuando inicia una instancia, mientras se encuentre en ejecución o cuando está detenida (en el caso de las instancias respaldadas por Amazon EBS).

El atributo `DisableApiTermination` no evita que termine una instancia cuando comienza el cierre desde la instancia (con un comando del sistema operativo para el cierre del sistema) cuando el atributo `InstanceInitiatedShutdownBehavior` está establecido. Para obtener más información, consulte Cambiar el comportamiento de apagado iniciado por la instancia.

Consideraciones

- La habilitación de la protección contra terminación no impide que AWS termine la instancia cuando hay un evento programado para terminar la instancia.
- La habilitación de la protección contra terminación no impide que Amazon EC2 Auto Scaling termine una instancia cuando la instancia no está en buen estado o durante eventos de reducción horizontal. Es posible controlar si un grupo de escalado automático puede terminar una instancia

en particular durante el proceso de escalado al usar la protección contra reducción horizontal de instancias. Puede controlar si un grupo de escalado automático puede terminar las instancias en mal estado al suspender el proceso de escalado de ReplaceUnhealthy.

- No puede habilitar la protección contra terminación para instancias de spot.

Para habilitar la protección contra terminación para una instancia en la inicialización

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel, elija Launch Instance (iniciar instancia) y siga las instrucciones del asistente.
3. En la página Configure Instance Details (Configurar detalles de instancia), seleccione la casilla de verificación Enable termination protection (Habilitar la protección de terminación).

Para habilitar la protección contra terminación para una instancia en ejecución o detenida

1. Seleccione la instancia y, a continuación, elija Actions (Acciones), Instance Settings (Configuración de instancia), Change Termination Protection (Cambiar protección de terminación).
2. Elija Yes, Enable (Sí, habilitar).

Para deshabilitar la protección contra terminación para una instancia en ejecución o detenida

1. Seleccione la instancia y, a continuación, elija Actions (Acciones), Instance Settings (Configuración de instancia), Change Termination Protection (Cambiar protección de terminación).
2. Elija Yes, Disable (Sí, deshabilitar).

Para habilitar o deshabilitar la protección contra terminación en la línea de comandos

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

- modify-instance-attribute (AWS CLI)
- Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

Terminación de varias instancias con la protección contra la terminación

Si termina varias instancias en varias zonas de disponibilidad en la misma solicitud, y una o más de las instancias especificadas están habilitadas para la protección de terminación, la solicitud falla con los siguientes resultados:

- Las instancias especificadas que se encuentran en la misma zona de disponibilidad que la instancia protegida no se terminan.
- Las instancias especificadas que se encuentran en diferentes zonas de disponibilidad, en las que no hay otras instancias especificadas protegidas, se terminan correctamente.

Ejemplo

Suponga que tiene las siguientes cuatro instancias en dos zonas de disponibilidad.

instancia	Zona de disponibilidad	Protección contra la terminación
Instancia 1	AZ A	`Disabled`
Instancia 2		`Disabled`
Instancia 3	AZ B	`Enabled`
Instancia 4		`Disabled`

Si se intenta terminar todas estas instancias en la misma solicitud, se informa de un error en la solicitud con los siguientes resultados:

- La instancia 1 y la instancia 2 se terminan con éxito porque ninguna de las instancias está habilitada para la protección de terminación.
- La instancia 3 y la instancia 4 no terminan porque la instancia 3 está habilitada para la protección de terminación.

Cambiar el comportamiento de apagado iniciado por la instancia

De manera predeterminada, cuando se inicia un cierre desde una instancia respaldada por Amazon EBS (mediante comandos como shutdown o poweroff), la instancia se detiene. Puede

cambiar este comportamiento para que la instancia termine en su lugar al cambiar el atributo `InstanceInitiatedShutdownBehavior` de la instancia. Puede cambiar este atributo mientras la instancia está en ejecución o detenida.

El comando halt no inicia un cierre. Si se usa, la instancia no termina; en su lugar, coloca la CPU en `HLT` y la instancia permanece en ejecución.

> **Note**
>
> El atributo `InstanceInitiatedShutdownBehavior` solo se aplica cuando se realiza un cierre desde el sistema operativo de la instancia en sí. No se aplica cuando se detiene una instancia mediante la API `StopInstances` o la consola de Amazon EC2.

Puede cambiar el atributo `InstanceInitiatedShutdownBehavior` con la línea de comandos o la consola de Amazon EC2.

Console

Para cambiar el comportamiento de cierre iniciado por la instancia

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instancias.
3. Seleccione la instancia.
4. Elija Actions (Acciones), Instance settings (Configuración de instancia), Change shutdown behavior (Cambiar comportamiento de cierre).

   El comportamiento de cierre muestra el comportamiento actual.
5. Para cambiar el comportamiento, en Comportamiento de cierre, seleccione Detener o Terminar.
6. Seleccione Guardar.

Command line

Para cambiar el comportamiento de cierre iniciado por la instancia

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

- modify-instance-attribute (AWS CLI)
- Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

Conservación de los datos cuando se termina una instancia

Según su caso de uso, es posible que desee conservar los datos del volumen de su almacén de instancias o del volumen de Amazon EBS cuando se termina la instancia de Amazon EC2. Los datos que hay en un volumen de almacén de instancias no persisten cuando se termina una instancia. Si necesita conservar los datos almacenados en un volumen de almacén de instancias más allá de la vida útil de la instancia, debe copiarlos manualmente a un almacenamiento más persistente, como un volumen de Amazon EBS, un bucket de Amazon S3 o un sistema de archivos de Amazon EFS. Para obtener más información, consulte Opciones de almacenamiento para sus instancias de Amazon EC2.

Para los datos de volumen de Amazon EBS, Amazon EC2 usa el valor del atributo `DeleteOnTermination` en cada volumen de Amazon EBS asociado para determinar si conservarlo o eliminarlo.

El valor predeterminado del atributo `DeleteOnTermination` varía dependiendo de si el volumen es el volumen raíz de la instancia o un volumen no raíz asociado a la instancia.

Volumen raíz

Por defecto, al inicializar una instancia, el atributo `DeleteOnTermination` para el volumen raíz de una instancia se establece en `true`. Por tanto, la opción predeterminada es eliminar el volumen raíz de la instancia cuando la instancia se termina.

Volumen no raíz

De manera predeterminada, cuando se adjunta un volumen no raíz de EBS a una instancia, su atributo `DeleteOnTermination` se establece en `false`. Por consiguiente, el valor predeterminado es conservar estos volúmenes.

> **Note**
>
> Después de que la instancia se termine, puede hacer una instantánea del volumen conservado o adjuntarlo a otra instancia. Para evitar incurrir en más cargos, debe eliminar el volumen.

El atributo `DeleteOnTermination` lo puede definir el creador de una AMI o la persona que inicia una instancia. Cuando el creador de una AMI o la persona que inicia una instancia cambia el atributo, la nueva configuración invalida la configuración predeterminada original de la AMI. Es recomendable que verifique la configuración predeterminada del atributo `DeleteOnTermination` después de iniciar una instancia con una AMI.

Para verificar si un volumen de Amazon EBS se eliminará cuando se termine la instancia, consulte los detalles del volumen en el panel de detalles de la instancia. En la pestaña de Storage (Almacenamiento), en Block devices (Dispositivos de bloques), desplácese hacia la derecha a fin de ver la configuración Delete on termination (Eliminar al terminar) para el volumen.

- Si la respuesta es Sí, el volumen se eliminará cuando se termine la instancia.
- Si la respuesta es No, el volumen no se eliminará cuando se termine la instancia. Los volúmenes que no se eliminen tras la terminación de la instancia seguirán incurriendo en cargos.

Cambio del volumen raíz para que persista en la inicialización

Utilizando la consola, puede cambiar el atributo `DeleteOnTermination` al iniciar una instancia. Para cambiar este atributo en una instancia en ejecución, debe utilizar la línea de comandos.

Use uno de los siguientes métodos para cambiar el volumen raíz para que persista en la inicialización.

Console

Para cambiar el volumen raíz de una instancia a persistente en la inicialización con la consola

1. Siga el procedimiento para iniciar una instancia, pero no la lance hasta que haya completado los siguientes pasos para cambiar el volumen raíz de modo que persista.
2. En Almacenamiento (volúmenes), amplíe la información que se encuentra debajo del volumen raíz.
3. En Eliminar al terminar, elija No.
4. En el panel Summary (Resumen), revise la configuración de la instancia y, a continuación, elija Launch instance (iniciar instancia). Para obtener más información, consulte Lance una instancia con el nuevo asistente de inicialización de instancias.

Command line

Cambiar el volumen raíz de una instancia para que persista en la inicialización con la línea de comandos

Cuando inicia una instancia con respaldo en EBS, puede usar uno de los comandos siguientes para cambiar el volumen de dispositivo raíz a persistente. Para obtener más información acerca de estas interfaces de línea de comandos, consulte Acceder a Amazon EC2.

- run-instances (AWS CLI)
- New-EC2Instance (AWS Tools for Windows PowerShell)

En las asignaciones de dispositivos de bloques para los volúmenes que desee conservar, incluya `--DeleteOnTermination` y especifique `false`.

Por ejemplo, para conservar un volumen, agregue la siguiente opción al comando `run-instances`:

```
--block-device-mappings file://mapping.json
```

En `mapping.json`, especifique el nombre del dispositivo (por ejemplo, `/dev/sda1` o `/dev/xvda`), y en lo que respecta a `--DeleteOnTermination`, especifique `false`.

```
[
  {
    "DeviceName": "device_name",
    "Ebs": {
      "DeleteOnTermination": false
    }
  }
]
```

Cambio del volumen raíz de una instancia en ejecución para que persista

Puede usar uno de los comandos siguientes para cambiar el volumen de dispositivo raíz de una instancia con respaldo en EBS en ejecución a persistente. Para obtener más información acerca de estas interfaces de línea de comandos, consulte Acceder a Amazon EC2.

- modify-instance-attribute (AWS CLI)

- Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

Por ejemplo, use el siguiente comando:

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --block-device-mappings file://mapping.json
```

En `mapping.json`, especifique el nombre del dispositivo (por ejemplo, `/dev/sda1` o `/dev/xvda`), y en lo que respecta a `--DeleteOnTermination`, especifique `false`.

```
[
  {
    "DeviceName": "device_name",
    "Ebs": {
      "DeleteOnTermination": false
    }
  }
]
```

Retirada de instancias

Una instancia se programa para retirarse cuando AWS detecta un error irreparable del hardware subyacente en el que se aloja la instancia. El dispositivo raíz de la instancia determina el comportamiento de la retirada de la instancia:

- Si el dispositivo raíz de la instancia es un volumen de Amazon EBS, la instancia se detiene y puede volver a iniciarla en cualquier momento. El comienzo de la instancia detenida la migra a hardware nuevo.
- Si el dispositivo raíz de la instancia es un volumen de almacén de instancias, la instancia se termina y no puede volver a utilizarse.

Para obtener más información acerca de los tipos de eventos de instancia, consulte Eventos programados para las instancias.

Contenido

- Identificar las instancias programadas para la retirada
- Acciones que se deben ejecutar en instancias respaldadas por EBS programadas para su retirada

- Acciones que se deben ejecutar en instancias respaldadas por almacenes de instancias programadas para su retirada

Identificar las instancias programadas para la retirada

Si la instancia está programada para retirada, recibirá un correo electrónico antes del evento con el ID de la instancia y la fecha de la retirada. También puede comprobar si hay instancias programadas para la retirada mediante la consola de Amazon EC2 o la línea de comandos.

> **Important**
>
> Si una instancia está programada para la retirada, le recomendamos que tome medidas lo antes posible, ya que es posible que sea inaccesible. (La notificación por correo electrónico que recibe indica lo siguiente: “Debido a esta degradación, puede que su instancia ya sea inaccesible”). Para obtener más información sobre la acción recomendada que debe realizar, consulte Check if your instance is reachable.

Formas de identificar las instancias programadas para la retirada

- Notificación por correo electrónico
- Identificación de la consola

Notificación por correo electrónico

Si la instancia está programada para retirada, recibirá un correo electrónico antes del evento con el ID de la instancia y la fecha de la retirada.

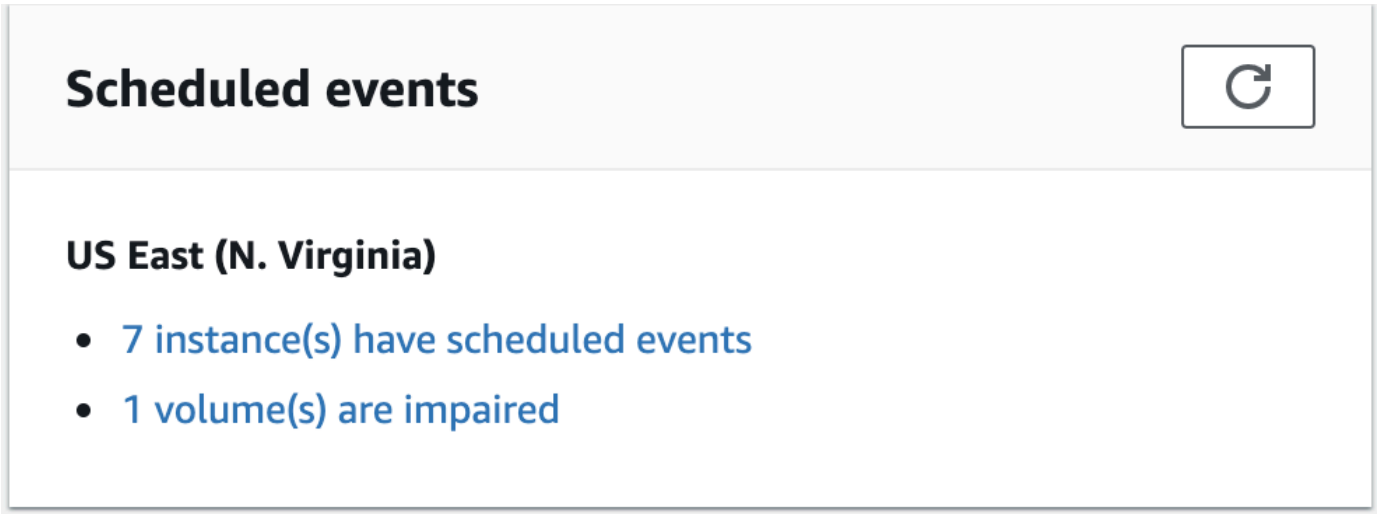
El correo electrónico se envía al titular de la cuenta principal y al contacto de operaciones. Para obtener más información, consulte Agregar, cambiar o quitar contactos alternativos en la Guía del usuario de AWS Billing.

Identificación de la consola

Si utiliza una cuenta de correo electrónico que no consulte con regularidad para las notificaciones de retirada de instancias, puede utilizar la consola de Amazon EC2 o la línea de comandos para determinar si alguna de las instancias está programada para la retirada.

Para identificar las instancias programadas para retirada con la consola

1. Abra la consola de Amazon EC2.
2. En el panel de navegación, elija EC2 Dashboard (Panel EC2). En Scheduled events (Eventos programados), puede consultar los eventos asociados con las instancias y volúmenes de Amazon EC2, organizados por región.



3. Si tiene una instancia con un evento programado en la lista, seleccione su vínculo bajo el nombre de la región para ir a la página Events (Eventos).
4. En la página Events (Eventos) se muestran todos los recursos que tienen eventos asociados. Para ver las instancias programadas para retirada, seleccione Instance resources (Recursos de instancia) en la primero lista de filtros y después Instance stop or retirement (Detención o retirada de instancias) en la segunda lista de filtros.
5. Si los resultados del filtro muestran que hay una instancia programada para retirada, selecciónela y observe la fecha y la hora en el campo Start time (Hora de inicio) en la página de detalles. Esta es la fecha de retirada de la instancia.

Para identificar las instancias programadas para retirada 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 Acceder a Amazon EC2.

- describe-instance-status (AWS CLI)
- Get-EC2InstanceStatus (AWS Tools for Windows PowerShell)

Acciones que se deben ejecutar en instancias respaldadas por EBS programadas para su retirada

Para conservar los datos de la instancia que se retira, puede realizar una de las siguientes acciones. Es importante que lo haga antes de la fecha de retirada de la instancia para evitar tiempo de inactividad imprevisto y pérdida de datos.

Para instancias de Linux, si no está seguro de si su instancia está respaldada por EBS o por el almacén de instancias, consulte Determinación del tipo de dispositivo raíz de la instancia de Linux.

Compruebe si su instancia es accesible

Cuando se le notifique que su instancia está programada para su retirada, le recomendamos que realice las siguientes acciones lo antes posible:

- Compruebe si su instancia es accesible conectándose o haciendo ping a ella.
- Si su instancia es accesible, debería planificar la detención/inicio de la instancia en un momento apropiado antes de la fecha de retirada programada, cuando el impacto sea mínimo. Para obtener más información acerca de la detención y comienzo de una instancia y de lo que sucede cuando se detiene, como el efecto en las direcciones IP elásticas privadas y públicas asociadas con la instancia, consulte Detención e iniciación de una instancia de Amazon EC2. Tenga en cuenta que los datos de los volúmenes de almacenamiento de instancias se pierden al detener y comenzar la instancia.
- Si su instancia es inaccesible, debe tomar medidas inmediatas y realizar una detención/inicio para recuperarla.
- De forma alternativa, si desea terminar su instancia, planifique hacerlo lo antes posible para que dejen de devengarse cargos por la instancia.

Crear una copia de seguridad de la instancia

Cree una AMI con respaldo en EBS a partir de la instancia para disponer de una copia de seguridad. Para garantizar la integridad de los datos, detenga la instancia antes de crear la AMI. Puede esperar a la fecha de retirada programada cuando la instancia se haya detenido o detenerla antes de la fecha de retirada. Puede iniciar la instancia de nuevo en cualquier momento. Para obtener más información, consulte Creación de una AMI basada en Amazon EBS.

iniciar una instancia de sustitución

Después de crear una AMI a partir de la instancia, puede utilizar la AMI para iniciar una instancia de sustitución. En la consola de Amazon EC2, seleccione su nueva AMI y, a continuación, elija Actions (Acciones), Launch (iniciar). Siga el asistente para iniciar la instancia. Para obtener más información acerca de cada paso del asistente, consulte Lance una instancia con el nuevo asistente de inicialización de instancias.

Acciones que se deben ejecutar en instancias respaldadas por almacenes de instancias programadas para su retirada

Para conservar los datos de la instancia que se retira, puede realizar una de las siguientes acciones. Es importante que lo haga antes de la fecha de retirada de la instancia para evitar tiempo de inactividad imprevisto y pérdida de datos.

> **Warning**
>
> Si la instancia con respaldo en el almacenamiento de la instancia cumple la fecha de retirada, se termina y no puede recuperarla y tampoco los datos que contuviera. Con independencia del dispositivo raíz de la instancia, los datos de los volúmenes con almacén de instancias se pierden cuando se retira la instancia, aunque estén asociados a una instancia con respaldo en EBS.

Comprobar si su instancia es accesible

Cuando se le notifique que su instancia está programada para su retirada, le recomendamos que realice las siguientes acciones lo antes posible:

- Compruebe si su instancia es accesible conectándose o haciendo ping a ella.
- Si su instancia es inaccesible, es probable que se pueda hacer muy poco para recuperarla. Para más información, consulte Solución de problemas de una instancia inaccesible. AWS terminará su instancia en la fecha de retiro programada, por lo que, en el caso de una instancia inaccesible, puede terminarla por su cuenta de inmediato.

iniciar una instancia de sustitución

Cree una AMI con respaldo en el almacenamiento de la instancia para la instancia utilizando las herramientas para AMI, tal y como se describe en Crear una AMI de Linux con respaldo en el almacén de instancias. En la consola de Amazon EC2, seleccione su nueva AMI y, a continuación,

elija Actions (Acciones), Launch (iniciar). Siga el asistente para iniciar la instancia. Para obtener más información acerca de cada paso del asistente, consulte Lance una instancia con el nuevo asistente de inicialización de instancias.

Convertir su instancia en una instancia respaldada por EBS

Transfiera los datos a un volumen de EBS, realice una instantánea del volumen y, a continuación, cree la AMI a partir de la instantánea. Puede iniciar una instancia de reemplazo desde la nueva AMI. Para obtener más información, consulte Convertir la AMI con respaldo en el almacén de instancias a una AMI respaldada por Amazon EBS.

Resiliencia de las instancias

> **Important**
>
> La siguiente información se aplica a la configuración de las capacidades relacionadas con la recuperación en instancias en buen estado. Si actualmente tiene dificultades para acceder a su instancia, consulte Solucionar problemas de instancias de EC2.

En caso de que AWS determine que una instancia no está disponible debido a un problema de hardware subyacente, hay dos mecanismos que puede configurar en relación con la resiliencia de la instancia y que pueden restablecer la disponibilidad: la recuperación automática simplificada y la recuperación basada en acciones de Amazon CloudWatch. Este proceso se denomina recuperación de instancias.

Para que se lleve a cabo el proceso de recuperación de la instancia, se debe configurar o habilitar previamente al menos un mecanismo con los recursos compatibles. Cuando se inicia una instancia compatible, se habilita la recuperación automática simplificada de forma predeterminada.

Temas

- Información general sobre la recuperación de instancias
- Alternativas a la recuperación de instancias
- Configuración de la recuperación basada en acciones de CloudWatch
- Configuración de la recuperación automática simplificada

Información general sobre la recuperación de instancias

Los siguientes son algunos ejemplos de problemas de hardware subyacentes que podrían requerir la recuperación de instancias:

- Pérdida de conectividad de red
- Pérdida de potencia del sistema
- Problemas de software en el host físico
- Problemas de hardware en el host físico que afectan a la accesibilidad a la red

La instancia recuperada es idéntica a la instancia original, incluido lo siguiente:

- ID de instancia
- Direcciones IP públicas, privadas y elásticas
- Metadatos de instancia
- Grupo de ubicación
- Volúmenes de EBS adjuntos
- Zona de disponibilidad

Cuando la instancia se recupera correctamente, esta actúa como si se reiniciara de forma no planificada. En otras palabras, el contenido almacenado en la memoria volátil se pierde, los datos del almacén de instancias se borran y el tiempo de actividad del sistema operativo vuelve a empezar desde cero.

Para ayudar a evitar la pérdida de datos, le recomendamos que cree copias de seguridad de los datos valiosos con regularidad. Para obtener más información sobre las prácticas recomendadas en cuanto a las copias de seguridad y la recuperación para las instancias de Amazon EC2, consulte las Prácticas recomendadas de Amazon EC2.

Alternativas a la recuperación de instancias

Se pueden considerar las siguientes alternativas a la recuperación de instancias cuando se adaptan al caso de uso de sus instancias.

Grupos de escalado automático

Puede usar grupos de escalado automático para poder agrupar un conjunto de instancias para los fines de escalado y disponibilidad. En caso de que una instancia de un grupo de escalado automático deje de estar disponible, dicho grupo reemplazará (no recuperará) la instancia automáticamente. Para obtener más información, consulte Grupo de Amazon EC2 Auto Scaling en la Guía del usuario de Amazon EC2 Auto Scaling.

Amazon EBS Multi-Attach

Puede configurar Amazon EBS Multi-Attach para sus instancias a fin de permitir la conexión de varias instancias al mismo volumen de EBS. Cuando se combina con el software adecuado, esto permite habilitar la agrupación en clústeres de alta disponibilidad. Para ver un ejemplo de configuración con instancias de Linux, consulte Clustered storage simplified: GFS2 on Amazon EBS Multi-Attach enabled volumes en el blog sobre almacenamiento de AWS.

Configuración de la recuperación basada en acciones de CloudWatch

Important

- La siguiente información se aplica a la configuración de las capacidades relacionadas con la recuperación en instancias en buen estado. Si actualmente tiene dificultades para acceder a su instancia, consulte Solucionar problemas de instancias de EC2.
- Para que la carga de trabajo funcione correctamente tras una recuperación correcta, la instancia debe arrancar y aceptar el tráfico sin necesidad de intervención manual.

Puede configurar la recuperación basada en acciones de Amazon CloudWatch para añadir acciones de recuperación a las alarmas de Amazon CloudWatch. La recuperación basada en acciones de CloudWatch funciona con la métrica de `StatusCheckFailed_System`. La recuperación basada en acciones de CloudWatch informa con precisión la granularidad de los tiempos de respuesta de la recuperación y envía notificaciones de Amazon Simple Notification Service (Amazon SNS) sobre las acciones y los resultados de recuperación. Estas opciones de configuración permiten intentar recuperar las instancias con mayor rapidez y con un control más preciso de la respuesta a los eventos de error en la comprobación del estado del sistema en comparación con la recuperación automática simplificada. Para obtener más información sobre las opciones de CloudWatch disponibles, consulte Comprobaciones de estado para sus instancias.

La recuperación basada en acciones de Amazon CloudWatch no funciona durante los eventos de servicio en el AWS Health Dashboard. Para obtener más información, consulte the section called “Solución de problemas durante la recuperación basada en acciones de Amazon CloudWatch”.

Temas

- Requisitos y limitaciones de la recuperación basada en acciones de CloudWatch
- Configuración de la recuperación basada en acciones de CloudWatch
- Solución de problemas durante la recuperación basada en acciones de Amazon CloudWatch

Requisitos y limitaciones de la recuperación basada en acciones de CloudWatch

La recuperación basada en acciones de CloudWatch puede intentar recuperar una instancia si esta:

- Está en estado de `running`. Para obtener más información, consulte the section called “Ciclo de vida de la instancia”.
- Usa la tenencia de instancia `default` (bajo demanda) o `dedicated`. Para obtener más información, consulte the section called “Opciones de compra de instancias”.
- Es de un tipo de instancia para el que Amazon EC2 tiene capacidad disponible. En algunas situaciones, como las interrupciones importantes, no habrá capacidad suficiente disponible y es posible que algunos intentos de recuperación fallen.
- No usa la tenencia de instancias `dedicated`. En el caso de los hosts dedicados de Amazon EC2, puede utilizar la recuperación automática de hosts dedicados para recuperar automáticamente las instancias en mal estado.
- No usa un dispositivo Elastic Fabric Adapter.
- No forma parte de un grupo de escalado automático.
- No se encuentra actualmente en proceso de mantenimiento programado.
- Usa uno de los siguientes tipos de instancia:
  - De uso general: A1 | M3 | M4 | M5 | M5a | M5n | M5zn | M6a | M6g | M6i | M6in | M7a | M7g | M7i | M7i-flex | T1 | T2 | T3 | T3a | T4g
  - Optimizadas para la computación: C3 | C4 | C5 | C5a | C5n | C6a | C6g | C6gn | C6i | C6in | C7a | C7g | C7gn | C7i | C7i-flex
  - Optimizadas para memoria: R3 | R4 | R5 | R5a | R5b | R5n | R6a | R6g | R6i | R6in | R7a | R7g | R7i | R7iz | u-3tb1 | u-6tb1 | u-9tb1 | u-12tb1 | u-18tb1 | u-24tb1 | u7i-12tb | u7in-16tb | u7in-24tb | u7in-32tb | X1 | X1e | X2iezn

  - De computación acelerada: G3 | G3s | G5g | Inf1 | P2 | P3 | VT1
  - De computación de alto rendimiento Hpc6a | Hpc7a | Hpc7g
  - Instancias metal: cualquiera de los tipos anteriores que tengan el tamaño de instancia metal.
- Tiene volúmenes de almacén de instancias y usa uno de los siguientes tipos de instancia: M3 | C3 | R3 | X1 | X1e | X2idn | X2iedn

> ⚠ Warning
>
> - Los datos almacenados en volúmenes de almacén de instancias se perderán si se detiene la instancia. Para obtener más información sobre cómo detener una instancia, consulte the section called “Detención e inicio de instancias”.
> - En caso de que se produzca un error en la comprobación del estado del sistema, es posible que se pierdan los datos del almacén de instancias y de la asignación de dispositivos de bloques. Para estos tipos de instancias, puede considerar usar the section called “Cómo habilitar la protección contra la terminación”.
>
> Le recomendamos que cree copias de seguridad de los datos valiosos con regularidad. Para obtener información sobre las prácticas recomendadas en cuanto a las copias de seguridad y la recuperación para Amazon EC2, consulte las Prácticas recomendadas de Amazon EC2.

También puede utilizar la AWS Management Console o la AWS CLI para ver los tipos de instancias que son compatibles con la recuperación basada en acciones de CloudWatch.

Console

Para ver los tipos de instancias que admiten la recuperación basada en acciones de Amazon CloudWatch

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación izquierdo, elija Instance Types (Tipos de instancias).
3. En la barra de filtros, ingrese Auto Recovery support: true (Compatibilidad con la recuperación automática: verdadero). Como alternativa, a medida que ingrese los caracteres y aparezca el nombre del filtro, podrá seleccionarlo.

La tabla de Tipos de instancias muestra todos los tipos de instancias que admiten la recuperación basada en acciones de Amazon CloudWatch.

AWS CLI

Para ver los tipos de instancias que admiten la recuperación basada en acciones de Amazon CloudWatch

Utilice el comando describe-instance-types.

```
aws ec2 describe-instance-types --filters Name=auto-recovery-supported,Values=true
--query "InstanceTypes[*].[InstanceType]" --output text | sort
```

Configuración de la recuperación basada en acciones de CloudWatch

La recuperación basada en acciones de CloudWatch funciona con la métrica de `StatusCheckFailed_System`. La recuperación basada en acciones de CloudWatch se configura mediante la consola de CloudWatch. Para configurar la recuperación basada en acciones de CloudWatch, consulte Adding recover actions to CloudWatch alarms en la Guía del usuario de Amazon CloudWatch.

Solución de problemas durante la recuperación basada en acciones de Amazon CloudWatch

Los siguientes problemas pueden hacer que se produzca un error en la recuperación de instancias con CloudWatch:

- La recuperación basada en acciones de CloudWatch no funciona durante los eventos de servicio en el AWS Health Dashboard. Es posible que no reciba notificaciones de error de recuperación de dichos eventos. Para obtener las últimas novedades sobre la disponibilidad del servicio, consulte la página de Estado del servicio.
- Capacidad temporal insuficiente de hardware de sustitución.
- La instancia ha alcanzado el límite máximo diario de tres intentos de recuperación. La instancia puede ser retirada si la recuperación automática da error y se determina que una degradación de hardware es la causa del error de comprobación de estado del sistema.

Si el error de comprobación del estado del sistema de la instancia continúa a pesar de haber hecho varios intentos de recuperarla, consulte Solucionar problemas de las instancias con comprobaciones de estado no superadas para obtener más información.

Configuración de la recuperación automática simplificada

> **Important**
>
> - La siguiente información se aplica a la configuración de las capacidades relacionadas con la recuperación en instancias en buen estado. Si actualmente tiene dificultades para acceder a su instancia, consulte Solucionar problemas de instancias de EC2.
> - Para que la carga de trabajo funcione correctamente tras una recuperación correcta, la instancia debe arrancar y aceptar el tráfico sin necesidad de intervención manual.

La recuperación automática simplificada controla todas las instancias en ejecución compatibles de forma predeterminada. Si se detecta un error en la comprobación del estado del sistema, la recuperación automática simplificada intenta corregir la instancia. La recuperación automática simplificada no funciona durante los eventos de servicio en el AWS Health Dashboard. Para obtener más información, consulte the section called “Solución de problemas durante la recuperación automática simplificada”.

Cuando ocurra un evento de recuperación automática simplificada, recibirá un evento del AWS Health Dashboard. Para configurar las notificaciones de estos eventos, consulte la sección Introducción a AWS User Notifications en la Guía del usuario de AWS User Notifications. También, puede utilizar las reglas de Amazon EventBridge para supervisar los eventos de recuperación automática simplificados mediante los siguientes códigos de evento:

- `AWS_EC2_SIMPLIFIED_AUTO_RECOVERY_SUCCESS`: eventos exitosos
- `AWS_EC2_SIMPLIFIED_AUTO_RECOVERY_FAILURE`: eventos fallidos

Para obtener más información, consulte Reglas de Amazon EventBridge.

Temas

- Requisitos y limitaciones de la recuperación automática simplificada
- Configuración de la recuperación automática simplificada

- Solución de problemas durante la recuperación automática simplificada

Requisitos y limitaciones de la recuperación automática simplificada

La recuperación automática simplificada intentará recuperar una instancia si esta:

- Está en estado de `running`. Para obtener más información, consulte the section called “Ciclo de vida de la instancia”.
- Usa la tenencia de instancia `default` (bajo demanda) o `dedicated`. Para obtener más información, consulte the section called “Opciones de compra de instancias”.
- Es de un tipo de instancia para el que Amazon EC2 tiene capacidad disponible. En algunas situaciones, como las interrupciones importantes, no habrá capacidad suficiente disponible y es posible que algunos intentos de recuperación fallen.
- No usa la tenencia de instancias `dedicated`. En el caso de los hosts dedicados de Amazon EC2, puede utilizar la recuperación automática de hosts dedicados para recuperar automáticamente las instancias en mal estado.
- No usa un dispositivo Elastic Fabric Adapter.
- No es una instancia de tamaño `metal`.
- No forma parte de un grupo de escalado automático.
- No se encuentra actualmente en proceso de mantenimiento programado.
- No tiene volúmenes de almacén de instancias.
- Usa uno de los siguientes tipos de instancia:
  - De uso general: A1 | M3 | M4 | M5 | M5a | M5n | M5zn | M6a | M6g | M6i | M6in | M7a | M7g | M7i | M7i-flex | T1 | T2 | T3 | T3a | T4g
  - Optimizadas para la computación: C3 | C4 | C5 | C5a | C5n | C6a | C6g | C6gn | C6i | C6in | C7a | C7g | C7gn | C7i | C7i-flex
  - Optimizadas para memoria: R3 | R4 | R5 | R5a | R5b | R5n | R6a | R6g | R6i | R6in | R7a | R7g | R7i | R7iz | u-3tb1 | u-6tb1 | u-9tb1 | u-12tb1 | u-18tb1 | u-24tb1 | u7i-12tb | u7in-16tb | u7in-24tb | u7in-32tb | X1 | X1e | X2iezn
  - De computación acelerada: G3 | G3s | G5g | Inf1 | P2 | P3 | VT1
  - De computación de alto rendimiento Hpc6a | Hpc7a | Hpc7g

⚠ Warning

- Los datos almacenados en volúmenes de almacén de instancias se perderán si se detiene la instancia. Para obtener más información sobre cómo detener una instancia, consulte the section called “Detención e inicio de instancias”.
- En caso de que se produzca un error en la comprobación del estado del sistema, es posible que se pierdan los datos del almacén de instancias y de la asignación de dispositivos de bloques. Para estos tipos de instancias, puede considerar usar the section called “Cómo habilitar la protección contra la terminación”.

Le recomendamos que cree copias de seguridad de los datos valiosos con regularidad. Para obtener información sobre las prácticas recomendadas en cuanto a las copias de seguridad y la recuperación para Amazon EC2, consulte las Prácticas recomendadas de Amazon EC2.

Configuración de la recuperación automática simplificada

Cuando inicia una instancia compatible, se habilita la recuperación automática simplificada de forma predeterminada. Puede configurar el comportamiento de la recuperación automática en `disabled` después de iniciar la instancia. La configuración `default` no habilita la recuperación automática simplificada para tipos de instancia no compatibles.

Console

Para desactivar la recuperación automática simplificada durante la instancia de inicialización

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instances (instancia[s]) y elija Launch Instances (iniciar instancias).
3. En la sección Advanced details (Detalles avanzados), en Instance auto-recovery (Recuperación automática de instancias), seleccione Disabled (Desactivado).
4. Configure los ajustes de inicialización de instancias restantes según sea necesario y luego lance la instancia.

Para deshabilitar la recuperación automática simplificada para una instancia en ejecución o detenida

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Seleccione la instancia y, a continuación, elija Actions (Acciones), Instance Settings (Configuración de la instancia), Change auto-recovery behavior (Cambiar comportamiento de recuperación automática).
4. Elija Off (Apagado) y, a continuación, elija Save (Guardar).

Para establecer el comportamiento de recuperación automática como **`default`** para una instancia en ejecución o detenida

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Seleccione la instancia y, a continuación, elija Actions (Acciones), Instance Settings (Configuración de la instancia), Change auto-recovery behavior (Cambiar comportamiento de recuperación automática).
4. Elija Predeterminado (activado) y, a continuación, elija Guardar.

AWS CLI

Para deshabilitar la recuperación automática simplificada durante la inicialización

Utilice el comando run-instances.

```
aws ec2 run-instances \
--image-id ami-1a2b3c4d \
--instance-type t2.micro \
--key-name MyKeyPair \
--maintenance-options AutoRecovery=Disabled \
  [...]
```

Para deshabilitar la recuperación automática simplificada para una instancia en ejecución o detenida

Utilice el comando modify-instance-maintenance-options.

```
aws ec2 modify-instance-maintenance-options \
--instance-id i-0abcdef1234567890 \
--auto-recovery disabled
```

Para establecer el comportamiento de recuperación automática como **`default`** para una instancia en ejecución o detenida

Utilice el comando modify-instance-maintenance-options.

```
aws ec2 modify-instance-maintenance-options \
--instance-id i-0abcdef1234567890 \
--auto-recovery default
```

Solución de problemas durante la recuperación automática simplificada

Los siguientes problemas pueden hacer que se produzca un error en la recuperación automática simplificada de la instancia:

- La recuperación automática simplificada no funciona durante los eventos de servicio en el AWS Health Dashboard. Es posible que no reciba notificaciones de error de recuperación de dichos eventos. Para obtener las últimas novedades sobre la disponibilidad del servicio, consulte la página de Estado del servicio.
- Capacidad temporal insuficiente de hardware de sustitución.
- La instancia ha alcanzado el límite máximo diario de tres intentos de recuperación. La instancia puede ser retirada si la recuperación automática da error y se determina que una degradación de hardware es la causa del error de comprobación de estado del sistema.

Si el error de comprobación del estado del sistema de la instancia continúa a pesar de haber hecho varios intentos de recuperarla, consulte Solucionar problemas de las instancias con comprobaciones de estado no superadas para obtener más información.

Trabajar con metadatos de instancias

Los metadatos de instancia son datos sobre una instancia que se pueden utilizar para configurar o administrar la instancia en ejecución. Los metadatos de instancia se dividen en categorías, como, por ejemplo, nombre de host, eventos y grupos de seguridad.

También puede utilizar metadatos de instancia para obtener acceso a los datos de usuario que ha especificado al iniciar la instancia. Por ejemplo, se pueden especificar parámetros para configurar la instancia o incluir un script sencillo. También puede crear AMI genéricas y usar los datos de usuario para modificar los archivos de configuración proporcionados durante la inicialización. Por ejemplo, si ejecuta servidores web para varios negocios pequeños, todos pueden utilizar la misma AMI genérica y recuperar el contenido de un bucket de Amazon S3 que especifique en los datos de usuario en la inicialización. Para añadir un nuevo cliente en cualquier momento, cree un bucket para el cliente, añada su contenido y lance la AMI con el nombre de bucket único proporcionado a su código en los datos de usuario. Si inicia varias instancias con la misma llamada a `RunInstances`, los datos de usuario se encuentran disponibles para todas las instancias de esa reserva. Cada instancia que forme parte de la misma reserva tiene un número `ami-launch-index` único para que pueda escribir código que controla lo que hacen las instancias. Por ejemplo, el primer host se puede elegir a sí mismo como el nodo original de un clúster. Para ver un ejemplo de inicialización de AMI detallado, consulte Ejemplo de Linux: valor de índice de inicialización de AMI.

Las instancias de EC2 también pueden incluir datos dinámicos, como, por ejemplo, un documento de identidad de instancia que se genera cuando se inicia la instancia. Para obtener más información, consulte Categorías de datos dinámicos.

> **Important**
>
> Aunque solo se puede obtener acceso a los metadatos de instancia y a los datos de usuario desde la propia instancia, los datos no están protegidos con métodos criptográficos ni de autenticación. Cualquier persona con acceso directo a la instancia, y prácticamente cualquier software que se ejecute en la instancia, puede ver sus metadatos. Por ello, no debería almacenar información confidencial, como contraseñas y claves de cifrado de duración prolongada, como datos de usuario.

Contenido

- Ejemplo de Linux: valor de índice de inicialización de AMI
- Documentos de identidad de instancias
- Roles de identidad de instancia

Utilizar IMDSv2

Para acceder a los metadatos de instancia desde una instancia en ejecución puede utilizar uno de los métodos siguientes:

- Servicio de metadatos de instancia, versión 1 (IMDSv1): un método de solicitud y respuesta
- Servicio de metadatos de instancia, versión 2 (IMDSv2): un método orientado a la sesión

De forma predeterminada, puede usar IMDSv1 o IMDSv2, o ambos.

Puede configurar el servicio de metadatos de instancia (IMDS) en cada instancia para que el código local o los usuarios deban usar IMDSv2. Si especifica que debe usarse IMDSv2, IMDSv1 dejará de funcionar. Para obtener información acerca de cómo configurar la instancia para usar IMDSv2, consulte Configurar las opciones de metadatos de instancia.

Los encabezados `PUT` o `GET` son exclusivos de IMDSv2. Si estas cabeceras están presentes en la solicitud, entonces la solicitud está destinada a IMDSv2. Si no hay encabezados, se supone que la solicitud está destinada a IMDSv1.

Para obtener más información, consulte Add defense in depth against open firewalls, reverse proxies, and SSRF vulnerabilities with enhancements to the EC2 Instance Metadata Service (Agregar defensa en profundidad contra firewalls abiertos, proxies inversos y vulnerabilidades SSRF con mejoras en el servicio de metadatos de instancias de EC2).

Para recuperar los metadatos de la instancia, consulte Recuperar metadatos de instancia.

Temas

- Funcionamiento de Servicio de metadatos de instancia versión 2
- Transición al uso de Servicio de metadatos de instancia, versión 2
- Uso de un AWS SDK compatible

Funcionamiento de Servicio de metadatos de instancia versión 2

IMDSv2 usa las solicitudes orientadas a la sesión. Las solicitudes orientadas a la sesión permiten crear un token de sesión que define la duración de la sesión, que puede ser de mínimo un segundo a un máximo de seis horas. En esa duración, puede utilizar el mismo token de sesión para solicitudes subsiguientes. Cuando la duración llegue a su fin, deberá crear un token de sesión nuevo para utilizarlo en las solicitudes futuras.

> **Note**
>
> En los ejemplos de esta sección, se utiliza la dirección IPv4 del servicio de metadatos de instancia (IMDS): `169.254.169.254`. Si recupera metadatos de instancia para las instancias de EC2 a través de la dirección IPv6, asegúrese de habilitar y utilizar la dirección IPv6 en su lugar: `[fd00:ec2::254]`. La dirección IPv6 de IMDS es compatible con los comandos de IMDSv2. Solo se puede acceder a la dirección IPv6 en instancias basadas en AWS Nitro System y en una subred compatible con IPv6 (de doble pila o solo IPv6).

En los siguientes ejemplos se usa un script de intérprete de comandos e IMDSv2 para recuperar los elementos de metadatos de instancias de nivel superior. Cada ejemplo:

- Crea un token de sesión que dura seis horas (21 600 segundos) con la solicitud `PUT`
- Almacena el encabezado del token de sesión en una variable denominada `TOKEN` (instancias de Linux) o `token` (instancias de Windows)
- Solicita los elementos de metadatos de nivel superior con el token

Ejemplo de Linux

Puede ejecutar dos comandos separados o combinarlos.

Comandos separados

Primero, genere un token con el siguiente comando.

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"`
```

A continuación, utilice el token para generar elementos de metadatos de nivel superior mediante el siguiente comando.

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
meta-data/
```

Comandos combinados

Puede almacenar el token y combinar los comandos. En el siguiente ejemplo se combinan los dos comandos anteriores y se almacena el encabezado del token de sesión en una variable denominada TOKEN.

> **Note**
>
> Si hay un error al crear el token, en lugar de un token válido, se almacena un mensaje de error en la variable y el comando no funcionará.

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-
ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/
```

Después de crear un token, puede volverlo a usar hasta que venza. En el siguiente comando de ejemplo, que toma el ID de la AMI utilizada para iniciar la instancia, se vuelve a utilizar el token que se almacena en `$TOKEN` en el ejemplo anterior.

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
meta-data/ami-id
```

Ejemplo de Windows

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -
Uri http://169.254.169.254/latest/meta-data/
```

Después de crear un token, puede volverlo a usar hasta que venza. En el siguiente comando de ejemplo, que toma el ID de la AMI utilizada para iniciar la instancia, se vuelve a utilizar el token que se almacena en `$token` en el ejemplo anterior.

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} `
```

```
-Method GET -uri http://169.254.169.254/latest/meta-data/ami-id
```

Al utilizar IMDSv2 para solicitar metadatos de instancia, la solicitud debe incluir lo siguiente:

1. Use una solicitud PUT para iniciar una sesión en el servicio de metadatos de instancia. La solicitud PUT devuelve un token que debe incluirse en las solicitudes GET subsiguientes del servicio de metadatos de instancia. El token debe acceder a los metadatos con IMDSv2.
2. Incluya el token en todas las solicitudes GET en IMDS. Cuando el uso del token se establece en `required`, las solicitudes sin un token válido o con un token que ha vencido reciben un código de error HTTP `401 - Unauthorized`.
   - El token es una clave específica de la instancia. El token no es válido en otras instancias de EC2 y se rechazará si intenta usarlo fuera de la instancia en la que se generó.
   - La solicitud PUT debe incluir un encabezado que especifique el tiempo de vida (TTL) del token, en segundos, de un máximo de seis horas (21 600 segundos). El token representa una sesión lógica. El TTL especifica el período de tiempo que es válido el token y, en consecuencia, la duración de la sesión.
   - Cuando un token caduca, para poder seguir accediendo a los metadatos de instancia hay que crear una sesión nueva con otro PUT.
   - Puede escoger entre volver a utilizar un token o crear uno nuevo con cada solicitud. Para una cantidad pequeña de solicitudes, puede ser más sencillo generar y usar inmediatamente un token cada vez que necesite acceder a IMDS. Pero para ser más eficientes, puede especificar una duración más larga para el token y volver a usarlo en vez de escribir una solicitud PUT cada vez que tenga que solicitar metadatos de instancia. No existe ningún límite práctico en cuanto a la cantidad de tokens simultáneos, cada uno de los cuales representa su propia sesión. Sin embargo, IMDSv2 sigue limitado por la conexión normal de IMDS y la limitación controlada. Para obtener más información, consulte Limitación de consultas.

Los métodos HTTP GET y HEAD están permitidos en las solicitudes de metadatos de instancia IMDSv2. Las solicitudes PUT se rechazan si contienen un encabezado X-Forwarded-For.

De forma predeterminada, la respuesta a las solicitudes PUT tiene un límite de saltos de respuesta (tiempo de vida) de 1 en el nivel del protocolo IP. Si necesita un límite de saltos mayor, puede ajustarlo con el comando modify-instance-metadata-options de AWS CLI. Por ejemplo, puede necesitar un límite de saltos mayor para una compatibilidad con versiones anteriores con servicios de contenedor ejecutándose en la instancia. Para obtener más información, consulte Configurar las opciones de metadatos para instancias existentes.

Transición al uso de Servicio de metadatos de instancia, versión 2

Al migrar a IMDSv2, le recomendamos que utilice las herramientas y la ruta de transición siguientes.

Temas

Herramientas para ayudar en la transición a IMDSv2

Si el software usa IMDSv1, utilice las siguientes herramientas a la hora de configurar el software para que use IMDSv2.

Software de AWS

Las últimas versiones de los SDK AWS CLI y AWS son compatibles con IMDSv2. Para usar IMDSv2, asegúrese de que las instancias de EC2 incluyan las versiones más recientes de los SDK y la CLI. Para obtener información acerca de cómo actualizar la CLI, consulte Instalar, actualizar y desinstalar AWS CLI en la Guía del usuario de AWS Command Line Interface.

Todos los paquetes de software de Amazon Linux 2 y Amazon Linux 2023 son compatibles con IMDSv2. En Amazon Linux 2023, IMDSv1 está deshabilitado de forma predeterminada.

Para conocer las versiones mínimas del AWS SDK compatibles con IMDSv2, consulte Uso de un AWS SDK compatible.

Analizador de paquetes IMDS

El analizador de paquetes IMDS es una herramienta de código abierto que identifica y registra las llamadas de IMDSv1 desde la fase de arranque de la instancia. Esto puede ayudar a identificar el software que realiza llamadas a IMDSv1 en las instancias de EC2, lo que le permitirá determinar exactamente lo que necesita actualizar para que sus instancias estén listas para usar únicamente IMDSv2. Puede ejecutar IMDS Packet Analyzer desde una línea de comandos o instalarlo como un servicio. Para obtener más información, consulta IMDS Packet Analyzer en GitHub.

CloudWatch

IMDSv2 utiliza sesiones respaldadas por tokens, mientras que IMDSv1 no. La métrica `MetadataNoToken` de CloudWatch realiza un seguimiento del número de llamadas al servicio de metadatos de instancia (IMDS) que están utilizando IMDSv1. Al seguir esta métrica hasta cero, puede determinar si y cuándo se ha actualizado el software para utilizar IMDSv2.

Tras inhabilitar IMDSv1, puede usar la métrica de CloudWatch `MetadataNoTokenRejected` para hacer un seguimiento del número de veces que se intentó y rechazó una llamada de IMDSv1. Al seguir esta métrica, puede determinar si es necesario actualizar el software para utilizar IMDSv2.

Para obtener más información, consulte Métricas de la instancia.

Actualizaciones de las API y las CLI de EC2

Para las instancias nuevas, puede usar la API RunInstances para iniciar instancias nuevas que exijan el uso de IMDSv2. Para obtener más información, consulte Configurar las opciones de metadatos para instancias nuevas.

En las instancias existentes, puede usar la API ModifyInstanceMetadataOptions para exigir el uso de IMDSv2. Para obtener más información, consulte Configurar las opciones de metadatos para instancias existentes.

Para requerir el uso de IMDSv2 en todas las instancias nuevas iniciadas por grupos de Auto Scaling, los grupos de Auto Scaling pueden utilizar una plantilla de inicialización o una configuración de inicialización. Al crear una plantilla de inicialización o crear una configuración de inicialización, debe configurar los parámetros `MetadataOptions` para requerir el uso de IMDSv2. El grupo de escalado automático inicia nuevas instancias con la nueva plantilla de inicialización o la configuración de inicialización, pero las instancias existentes no resultan afectadas. Para las instancias existentes en un grupo de escalado automático, puede utilizar la API ModifyInstanceMetadataOptions para requerir el uso de IMDSv2 en las instancias existentes o terminar las instancias y el grupo de escalado automático iniciará nuevas instancias de sustitución con la configuración de las opciones de metadatos de la instancia definida en la plantilla de inicialización o en la configuración de inicialización.

Utilice una AMI que configure IMDSv2 de forma predeterminada

Al iniciar una instancia, puede configurarla automáticamente para que utilice IMDSv2 de forma predeterminada (el parámetro `HttpTokens` se establece en `required`) al iniciarlo con una AMI que esté configurada con el parámetro `ImdsSupport` establecido en `v2.0`. Puede establecer el parámetro `ImdsSupport` en `v2.0` al registrar la AMI mediante el comando de CLI register-image o puede modificar una AMI existente mediante el comando de CLI modify-image-attribute. Para obtener más información, consulte Configuración de la AMI.

Políticas de IAM y SCP

Puede utilizar una política de IAM o una política de control de servicio (SCP) AWS Organizations para controlar a los usuarios de IAM de la siguiente forma:

- No se puede iniciar una instancia con la API RunInstances, a menos que la instancia esté configurada para usar IMDSv2.
- No se puede modificar una instancia en ejecución mediante la API ModifyInstanceMetadataOptions para volver a habilitar IMDSv1.

La política de IAM o SCP debe contener las siguientes claves de condición de IAM:

- `ec2:MetadataHttpEndpoint`
- `ec2:MetadataHttpPutResponseHopLimit`
- `ec2:MetadataHttpTokens`

Si un parámetro en la llamada API o CLI no coincide con el estado especificado en la política que contiene la clave de condición, la llamada API o CLI falla con una respuesta `UnauthorizedOperation`.

Además, puede elegir una capa de protección adicional para forzar el cambio de IMDSv1 a IMDSv2. En la capa de administración de acceso, en relación con las API que se han llamado con credenciales de rol de EC2, puede usar una clave de condición nueva en políticas de IAM o políticas de control de servicios (SCP) de AWS Organizations. En específico, al usar la clave de condición de política `ec2:RoleDelivery` con un valor `2.0` en las políticas de IAM, las llamadas a la API realizadas con credenciales de rol de EC2 que se han obtenido de IMDSv1 recibirán la respuesta `UnauthorizedOperation`. Se puede conseguir lo mismo de forma más extensa si dicha condición la exige una SCP. De esta manera se logra que las credenciales proporcionadas mediante IMDSv1 no se puedan usar para llamar a las API porque cualquier llamada a la API que no cumpla la condición especificada recibirá un error `UnauthorizedOperation`.

Para ver ejemplos de políticas de IAM, consulte Trabajar con metadatos de instancias. Para obtener más información sobre SCP, consulte Políticas de control de servicios en la Guía del usuario de AWS Organizations.

Ruta recomendada para exigir IMDSv2

Si se usan las herramientas anteriores, recomendamos seguir esta ruta para pasar a IMDSv2.

Paso 1: Al principio

Actualice los SDK, las CLI y su software que usan credenciales de rol en sus instancias de EC2 a versiones compatibles con IMDSv2. Para obtener más información sobre cómo actualizar CLI, consulte Actualizar a la versión más reciente de AWS CLI en la Guía del usuario de AWS Command Line Interface.

A continuación, cambie el software que accede directamente a los metadatos de instancia (en otras palabras, que no usan un SDK) con las solicitudes IMDSv2. Puede utilizar el analizador de paquetes IMDS para identificar el software que necesita cambiar para utilizar las solicitudes de IMDSv2.

Paso 2: haga un seguimiento del progreso de la transición

Realice un seguimiento del progreso de la transición utilizando la métrica de CloudWatch `MetadataNoToken`. Esta métrica muestra la cantidad de llamadas de IMDSv1 a IMDS de las instancias. Para obtener más información, consulte Métricas de la instancia.

Paso 3: cuando no hay uso de IMDSv1

Cuándo la métrica de CloudWatch `MetadataNoToken` no registra ningún uso de IMDSv1, las instancias están listas para la transición completa al uso de IMDSv2. En esta etapa, puede hacer lo siguiente:

- Cuenta predeterminada

  Puede configurar IMDSv2 para que sea un requisito predeterminado de la cuenta. Cuando se inicia una instancia, la configuración de la instancia se establece automáticamente en la cuenta predeterminada.

  Para configurar la cuenta predeterminada, haga lo siguiente:

  - Consola Amazon EC2: en el panel de EC2, en Atributos de la cuenta, Protección y seguridad de datos, para ver los valores predeterminados de IMDS, establezca el Servicio de metadatos de instancia en Habilitado y la Versión de metadatos en V2 únicamente (token obligatorio). Para obtener más información, consulte Ajuste de IMDSv2 como valor predeterminado de la cuenta.
  - AWS CLI: use el comando de la CLI modify-instance-metadata-defaults y especifique `--http-tokens required` y `--http-put-response-hop-limit 2`.
- instancias nuevas

  Al iniciar una nueva instancia, puede hacer lo siguiente:

  - Consola de Amazon EC2: En el asistente de instancia de inicialización, establezca Metadata accessible (Metadatos accesibles) en Enabled (Habilitados) y Metadata version (Versión de metadatos) en V2 only (token required) (Solo V2 [token necesario]). Para obtener más información, consulte Configuración de la instancia en el momento de la inicialización.
  - AWS CLI: use el comando de la CLI run-instances y especifique que solo se requiere IMDSv2.
- instancias existentes

  Para instancias existentes, puede hacer lo siguiente:

  - Consola de Amazon EC2: en la página instancias, seleccione su instancia, elija Acciones, Configuración de la instancia, Modificar las opciones de metadatos de la instancia y, para IMDSv2, elija Obligatorio. Para obtener más información, consulte Requerir el uso de IMDSv2.
  - AWS CLI: utilice el comando de la CLI modify-instance-metadata-options para especificar que solo se debe utilizar IMDSv2.

  Puede modificar las opciones de metadatos de las instancias en ejecución y no es necesario reiniciar las instancias después de modificar las opciones de metadatos de la instancia.

Paso 4: Comprobación de si todas las instancias han pasado a IMDSv2

Puede comprobar si alguna instancia aún no está configurada para requerir el uso de IMDSv2; en otras palabras, IMDSv2 sigue configurado como `optional`. Si alguna instancia sigue configurada como `optional`, puede modificar las opciones de metadatos de la instancia para hacer que IMDSv2 sea `required` mediante la repetición del paso 3 anterior.

Para filtrar las instancias, haga lo siguiente:

- Consola de Amazon EC2: en la página instancias, filtre las instancias mediante el filtro IMDSv2 = opcional. Para obtener más información sobre cómo filtrar, consulte Filtrar recursos mediante la consola. También puede ver si IMDSv2 es obligatorio u opcional para cada instancia. En la ventana Preferencias, active IMDSv2 para agregar la columna IMDSv2 a la tabla instancias.
- AWS CLI: utilice el comando de la CLI describe-instances y filtre por `metadata-options.http-tokens = optional`, de la siguiente manera:

```
aws ec2 describe-instances --filters "Name=metadata-options.http-
tokens,Values=optional" --query "Reservations[*].Instances[*].[InstanceId]" --output
 text
```

Paso 5: Cuando todas las instancias han pasado a IMDSv2

Las claves de condición de IAM `ec2:MetadataHttpTokens`, `ec2:MetadataHttpPutResponseHopLimit` y `ec2:MetadataHttpEndpoint` se pueden utilizar para controlar el uso de las API RunInstances y ModifyInstanceMetadataOptions, así como la CLI correspondiente. Si se crea una política y un parámetro en la llamada a la API no coincide con el estado especificado en la política que usa la clave de condición, la llamada a la API o a la CLI devolverá una respuesta de error `UnauthorizedOperation`. Para ver ejemplos de políticas de IAM, consulte Trabajar con metadatos de instancias.

Además, después de deshabilitar IMDSv1, puede usar la métrica de CloudWatch `MetadataNoTokenRejected` para hacer un seguimiento del número de veces que se intentó y rechazó una llamada de IMDSv1. Si, después de deshabilitar IMDSv1, tiene un software que no funciona correctamente y la métrica `MetadataNoTokenRejected` registra las llamadas de IMDSv1, es probable que este software deba actualizarse para usar IMDSv2.

Uso de un AWS SDK compatible

Para usar IMDSv2, las instancias de EC2 deben usar una versión de AWS SDK que admita el uso de IMDSv2. Las últimas versiones de todos los SDK de AWS son compatibles con IMDSv2.

> **Important**
>
> Le recomendamos que se mantenga al día con las versiones del SDK para estar al tanto de las características, las actualizaciones de seguridad y las dependencias subyacentes más recientes. No se recomienda el uso continuo de una versión del SDK no admitida, hágalo según su criterio. Para obtener más información, consulte Política de mantenimiento de SDK y herramientas de AWS en la Guía de referencia de SDK y herramientas de AWS.

Las siguientes son las versiones mínimas que admiten el uso de IMDSv2:

- AWS CLI: 1.16.289
- AWS Tools for Windows PowerShell— 4.0.1.0
- AWS SDK for .NET: 3.3.634.1
- AWS SDK for C++: 1.7.229
- AWS SDK for Go: 1.25.38
- AWS SDK para Go v2: 0.19.0

- AWS SDK for Java: 1.11.678
- AWS SDK for Java 2.x: 2.10.21
- AWS SDK para JavaScript en Node.js: 2.722.0
- AWS SDK for PHP: 3.147.7
- AWSSDK para Python (Botocore) – 1.13.25
- AWS SDK for Python (Boto3): 1.12.6
- AWS SDK for Ruby: 3.79.0

Configurar las opciones de metadatos de instancia

El servicio de metadatos de instancias (IMDS) se ejecuta de forma local en todas las instancias de EC2. Las opciones de metadatos de instancia hacen referencia a un conjunto de configuraciones que controlan la accesibilidad y el comportamiento del IMDS en una instancia de EC2.

Puede configurar las siguientes opciones de metadatos de instancia en cada instancia.

Servicio de metadatos de instancias (IMDS): `enabled` | `disabled`

Puede habilitar o deshabilitar el IMDS en una instancia. Si está deshabilitado, ni usted ni ningún código podrá acceder a los metadatos de la instancia.

El IMDS tiene dos puntos de conexión en una instancia: IPv4 (`169.254.169.254`) e IPv6 (`[fd00:ec2::254]`). Al habilitar el IMDS, el punto de conexión IPv4 se habilita automáticamente. Si desea habilitar el punto de conexión IPv6, tendrá que hacerlo de forma explícita.

Punto de conexión IPv6 del IMDS: `enabled` | `disabled`

Puede habilitar de forma explícita el punto de conexión IPv6 del IMDS en una instancia. Cuando el punto de conexión IPv6 está habilitado, el punto de conexión IPv4 permanece habilitado. El punto de conexión IPv6 solo es compatible con instancias basadas en AWS Nitro System y en una subred compatible con IPv6 (de doble pila o solo IPv6).

Versión de metadatos: `IMDSv1 or IMDSv2 (token optional)` | `IMDSv2 only (token required)`

Al solicitar metadatos de instancia, las llamadas de IMDSv2 solicitan un token. Las llamadas de IMDSv1 no requieren un token. Puede configurar una instancia para que permita las llamadas

de IMDSv1 o IMDSv2 (en las que el token es opcional) o para que solo permita las llamadas de IMDSv2 (en las que el token es obligatorio).

Límite de saltos de respuesta de metadatos: 1–64

El límite de saltos es el número de saltos de red que puede realizar la respuesta PUT. Puede establecer el límite de saltos en un mínimo de 1 y un máximo de 64. En un entorno de contenedores, recomendamos establecer el límite de saltos en 2. Para obtener más información, consulte Consideraciones.

Acceso a etiquetas en metadatos de instancia: `enabled` | `disabled`

Puede habilitar o deshabilitar el acceso a las etiquetas de la instancia desde los metadatos de instancia. Para obtener más información, consulte Trabajar con etiquetas de instancia en los metadatos de instancia.

Dónde configurar las opciones de metadatos de instancia

Las opciones de metadatos de instancia se pueden configurar en diferentes niveles, de la siguiente manera:

- Cuenta: puede establecer valores predeterminados para las opciones de metadatos de instancia a nivel de cuenta para cada Región de AWS. Cuando se inicia una instancia, las opciones de metadatos de instancia se configuran automáticamente en los valores a nivel de cuenta. Puede cambiar este valor en el momento de la inicialización. Los valores predeterminados a nivel de cuenta no afectan a las instancias existentes.
- AMI: puede establecer el parámetro `imds-support` a `v2.0` cuando registra o modifica una AMI. Cuando se inicia una instancia con esta AMI, la versión de metadatos de instancia se establece automáticamente en IMDSv2 y el límite de saltos se establece en 2.
- instancia: puede cambiar todas las opciones de metadatos de instancia en el momento de la inicialización, al anular la configuración predeterminada. También puede cambiar las opciones de metadatos de instancia después de la inicialización en una instancia en ejecución o detenida. Tenga en cuenta que los cambios pueden restringirse mediante una política de IAM o SCP.

Para obtener más información, consulte Configurar las opciones de metadatos para instancias nuevas y Configurar las opciones de metadatos para instancias existentes.

Orden de prioridad para las opciones de metadatos de instancia

El valor de cada opción de metadatos de instancia se determina en el momento de la inicialización de la instancia, siguiendo un orden jerárquico de prioridad. La jerarquía, con la prioridad más alta en la parte superior, es la siguiente:

- Prioridad 1, configuración de la instancia en la inicialización: los valores se pueden especificar en la plantilla de inicialización o en la configuración de la instancia. Todos los valores especificados aquí anulan los valores especificados a nivel de cuenta o en la AMI.
- Prioridad 2, configuración de la cuenta: si no se especifica un valor al iniciar la instancia, lo determina la configuración a nivel de cuenta (que se establece para cada Región de AWS). La configuración a nivel de cuenta incluye un valor para cada opción de metadatos o no indica ninguna preferencia.
- Prioridad 3, configuración de la AMI: si no se especifica un valor al iniciar la instancia o a nivel de cuenta, lo determina la configuración de la AMI. Esto se aplica solo a `HttpTokens` y `HttpPutResponseHopLimit`.

Cada opción de metadatos se evalúa por separado. La instancia se puede ajustar con una combinación de configuración de instancia directa, valores predeterminados a nivel de cuenta y la configuración de la AMI.

Puede cambiar el valor de cualquier opción de metadatos después de la inicialización en una instancia en ejecución o detenida, a menos que los cambios estén restringidos por una política de IAM o SCP.

Determine los valores de las opciones de metadatos: ejemplo 1

En este ejemplo, se inicia una instancia de EC2 en una Región en la que `HttpPutResponseHopLimit` se establece en 1 a nivel de cuenta. La AMI especificada tiene `ImdsSupport` establecido en `v2.0`. En el momento de la inicialización, no se especifican opciones de metadatos directamente en la instancia. La instancia se inicia con las siguientes opciones de metadatos:

```
"MetadataOptions": {
    ...
    "HttpTokens": "required",
    "HttpPutResponseHopLimit": 1,
    ...
```

Estos valores se determinaron de la siguiente manera:

- No se especificaron opciones de metadatos en el momento de la inicialización: durante la inicialización de la instancia, no se proporcionaron valores específicos para las opciones de metadatos ni en los parámetros de inicialización de la instancia ni en la plantilla de inicialización.
- La configuración de la cuenta tiene prioridad: si no se especifican valores específicos en el momento de la inicialización, prevalece la configuración a nivel de la cuenta dentro de la Región. Esto significa que se aplican los valores predeterminados configurados a nivel de cuenta. En este caso, `HttpPutResponseHopLimit` se estableció en `1`.
- La configuración de la AMI tiene prioridad: en ausencia de un valor específico en la inicialización o a nivel de cuenta para `HttpTokens` (la versión de metadatos de la instancia), se aplica la configuración de la AMI. En este caso, la configuración de AMI `ImdsSupport: v2.0` determinó que `HttpTokens` se estableció en `required`. Tenga en cuenta que, si bien la configuración de la AMI `ImdsSupport: v2.0` está diseñada para establecerse como `HttpPutResponseHopLimit: 2`, la configuración a nivel de cuenta `HttpPutResponseHopLimit: 1`, que tiene mayor prioridad, la anuló.

Determine los valores de las opciones de metadatos: ejemplo 2

En este ejemplo, la instancia de EC2 se inicia con la misma configuración que en el ejemplo 1 anterior, pero con `HttpTokens` configurados `optional` directamente como en la instancia en el momento de la inicialización. La instancia se inicia con las siguientes opciones de metadatos:

```
"MetadataOptions": {
    ...
    "HttpTokens": "optional",
    "HttpPutResponseHopLimit": 1,
    ...
```

El valor de `HttpPutResponseHopLimit` se determina de la misma manera que en el ejemplo 1. Sin embargo, el valor de `HttpTokens` se determina de la siguiente manera: las opciones de metadatos configuradas en la instancia en el momento de la inicialización tienen prioridad. Aunque la AMI se configuró con `ImdsSupport: v2.0` (en otras palabras, `HttpTokens` se establecieron como `required`), prevaleció el valor especificado en la instancia en el momento de la inicialización (`HttpTokens` se establecieron como `optional`).

Ajuste de la versión de los metadatos de instancia

Cuando se inicia una instancia, el valor de la versión de metadatos de la instancia es `IMDSv1 or IMDSv2 (token optional)` o `IMDSv2 only (token required)`.

Al iniciar la instancia, puede especificar de forma manual el valor de la versión de metadatos o usar el valor predeterminado. Si especifica el valor de forma manual, anulará los valores predeterminados. Si opta por no especificar el valor de forma manual, se determinará mediante una combinación de ajustes predeterminados, como se indica en la tabla siguiente.

En la tabla se muestra cómo se determina la versión de metadatos de una instancia en el momento de la inicialización (indicada en la columna 4, en la Configuración de la instancia resultante) en función de los ajustes de los distintos niveles de configuración. El orden de prioridad es de izquierda a derecha, donde la primera columna tiene mayor prioridad, como se indica a continuación:

- Columna 1: Parámetro de inicialización, representa la configuración de la instancia que se especifica de forma manual en la inicialización.
- Columna 2: Nivel de cuenta predeterminado, representa la configuración de la cuenta.
- Columna 3: Valor predeterminado de la AMI, representa la configuración de la AMI.

Parámetro de inicialización	Nivel de cuenta predeterminado	AMI predeterminada	Configuración de la instancia resultante
V2 únicamente (token obligatorio)	Sin preferencias	V2 únicamente	V2 únicamente
V2 únicamente (token obligatorio)	V2 únicamente	V2 únicamente	V2 únicamente
V2 únicamente (token obligatorio)	V1 o V2	V2 únicamente	V2 únicamente
V1 o V2 (token obligatorio)	Sin preferencias	V2 únicamente	V1 o V2
V1 o V2 (token obligatorio)	V2 únicamente	V2 únicamente	V1 o V2

Parámetro de inicialización	Nivel de cuenta predeterminado	AMI predeterminada	Configuración de la instancia resultante
V1 o V2 (token obligatorio)	V1 o V2	V2 únicamente	V1 o V2
No configurado	Sin preferencias	V2 únicamente	V2 únicamente
No configurado	V2 únicamente	V2 únicamente	V2 únicamente
No configurado	V1 o V2	V2 únicamente	V1 o V2
V2 únicamente (token obligatorio)	Sin preferencias	null	V2 únicamente
V2 únicamente (token obligatorio)	V2 únicamente	null	V2 únicamente
V2 únicamente (token obligatorio)	V1 o V2	null	V2 únicamente
V1 o V2 (token obligatorio)	Sin preferencias	null	V1 o V2
V1 o V2 (token obligatorio)	V2 únicamente	null	V1 o V2
V1 o V2 (token obligatorio)	V1 o V2	null	V1 o V2
No configurado	Sin preferencias	null	V1 o V2
No configurado	V2 únicamente	null	V2 únicamente
No configurado	V1 o V2	null	V1 o V2

Uso de las claves de condición de IAM para restringir las opciones de metadatos de instancia

Puede utilizar claves de condición de IAM en una política de IAM o SCP de la siguiente forma:

- Permitir que una instancia se lance únicamente si está configurada para requerir el uso de IMDSv2
- Restringir el número de saltos permitidos
- Desactivar el acceso a los metadatos de instancia

Tareas

- Configurar las opciones de metadatos para instancias nuevas
- Configurar las opciones de metadatos para instancias existentes

> **Note**
>
> Debe proceder con cautela y realizar pruebas antes de realizar cambios. Tome nota de lo siguiente:
>
> - Si fuerza el uso de IMDSv2, las aplicaciones o los agentes que usen IMDSv1 para acceder a metadatos de instancia se interrumpirán.
> - Si desactiva todo acceso a los metadatos de instancia, las aplicaciones o los agentes que confíen en que el acceso a metadatos de instancia funcione, se interrumpirán.
> - En el caso de IMDSv2, debe utilizar `/latest/api/token` al recuperar el token.
> - (Solo Windows) Si la versión de PowerShell es anterior a 4.0, debe actualizar a Windows Management Framework 4.0 para requerir el uso de IMDSv2.

Configurar las opciones de metadatos para instancias nuevas

Puede configurar las siguientes opciones de metadatos para nuevas instancias.

Opciones

- Requerir el uso de IMDSv2
- Habilitación de los puntos de conexión IPv4 e IPv6 de IMDS
- Desactivar el acceso a los metadatos de instancia

Requerir el uso de IMDSv2

Puede usar los siguientes métodos para exigir el uso de IMDSv2 en sus instancias nuevas.

Exigencia de IMDSv2

- Ajuste de IMDSv2 como valor predeterminado de la cuenta
- Configuración de la instancia en el momento de la inicialización
- Configuración de la AMI
- Uso de una política de IAM

Ajuste de IMDSv2 como valor predeterminado de la cuenta

Puede establecer el valor predeterminado del servicio de metadatos de instancias (IMDS) a nivel de cuenta para cada Región de AWS. Cuando se inicia una instancia nueva, la versión de metadatos de la instancia se configura automáticamente al valor a nivel de cuenta predeterminado. Sin embargo, puede anular el valor manualmente al iniciarla o después. Para obtener más información sobre cómo afectan a una instancia la configuración a nivel de cuenta y las anulaciones manuales, consulte Orden de prioridad para las opciones de metadatos de instancia

> **Note**
>
> Si se establece el valor predeterminado a nivel de cuenta, no se restablecen las instancias existentes. Por ejemplo, si establece el valor predeterminado a nivel de cuenta en IMDSv2, las instancias existentes que estén configuradas en IMDSv1 no se verán afectadas. Si desea cambiar el valor de las instancias existentes, debe cambiarlo manualmente en las propias instancias.

Puede establecer el valor predeterminado de la cuenta para la versión de metadatos de instancia en IMDSv2, de modo que todas las instancias nuevas de la cuenta se inicien con IMDSv2 obligatoriamente y, de esta forma, se deshabilita IMDSv1. Con esta cuenta predeterminada, cuando lance una instancia, los valores predeterminados de la instancia serán los siguientes:

- Consola: la versión de metadatos se configura en V2 únicamente (token obligatorio) y el límite de saltos de respuesta de los metadatos se establece en 2.
- AWS CLI: `HttpTokens` se configuran como `required` y `HttpPutResponseHopLimit` se configura en 2.

> **Note**
>
> Antes de establecer el valor predeterminado de la cuenta en IMDSv2, asegúrese de que las instancias no dependan de IMDSv1. Para obtener más información, consulte Ruta recomendada para exigir IMDSv2.

Console

Cómo configurar IMDSv2 como valor predeterminado para la cuenta de la Región especificada

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. En el panel de navegación, elija EC2 Dashboard (Panel EC2).
4. En Atributos de la cuenta, elija Protección y seguridad de datos.
5. Junto a los Valores predeterminados de IMDS, seleccione Administrar.
6. En la página Administrar valores predeterminados de IMDS, haga lo siguiente:
   a. En Servicio de metadatos de instancia, seleccione Habilitado.
   b. En Metadata version (Versión de metadatos), elija V2 only (token required) (solo V2 [token obligatorio]).
   c. En el Límite de saltos de respuesta de metadatos, especifique 2 si las instancias alojarán contenedores. De lo contrario, seleccione Sin preferencia. Si no se especifica ninguna preferencia, en el momento de la inicialización, el valor predeterminado será 2 si la AMI requiere IMDSv2; de lo contrario, el valor predeterminado será 1.
   d. Elija Actualizar.

AWS CLI

Cómo configurar IMDSv2 como valor predeterminado para la cuenta de la Región especificada

Use el comando modify-instance-metadata-defaults y especifique la Región en la que desea modificar la configuración a nivel de cuenta de IMDS. Incluya `--http-tokens` establecidos como `required` y `--http-put-response-hop-limit` establecido en 2 si las instancias alojarán contenedores. De lo contrario, especifique `-1` si no desea indicar ninguna preferencia.

Si `-1` (sin preferencia) se especifica, en el momento de la inicialización, el valor predeterminado será 2 si la AMI requiere IMDSv2; de lo contrario, el valor predeterminado será 1.

```
aws ec2 modify-instance-metadata-defaults \
    --region us-east-1 \
    --http-tokens required \
    --http-put-response-hop-limit 2
```

Resultado previsto

```
{
    "Return": true
}
```

Cómo ver la configuración de cuenta predeterminada para las opciones de metadatos de instancia para la Región especificada

Use el comando get-instance-metadata-defaults y especifique la Región.

```
aws ec2 get-instance-metadata-defaults --region us-east-1
```

Ejemplo de resultado

```
{
    "AccountLevel": {
        "HttpTokens": "required",
        "HttpPutResponseHopLimit": 2
    }
}
```

Configuración de la instancia en el momento de la inicialización

Al iniciar una instancia, puede configurarla para exigir el uso de IMDSv2 mediante la configuración de los siguientes campos:

- Consola de Amazon EC2: establezca Metadata version (Versión de metadatos) en V2 only (token required) (Solo V2 [token obligatorio]).
- AWS CLI: `HttpTokens` establecido en `required`.

Al especificar que IMDSv2 es obligatorio, también se debe habilitar el punto de conexión del servicio de metadatos de instancia (IMDS); para ello, se debe establecer Metadatos accesibles en Habilitados (consola) o `HttpEndpoint` en `enabled` (AWS CLI).

En un entorno de contenedores, cuando se requiere IMDSv2, recomendamos establecer el límite de saltos en 2. Para obtener más información, consulte Consideraciones.

New console

Para exigir el uso de IMDSv2 en una nueva instancia

- Al iniciar una nueva instancia en la consola de Amazon EC2, despliegue Advanced details (Detalles avanzados) y haga lo siguiente:
  - Para Metadatos accesibles, elija Enabled (Habilitado).
  - En Metadata version (Versión de metadatos), elija V2 only (token required) (solo V2 [token obligatorio]).
  - (Entorno de contenedores) Para el límite de saltos de respuesta de metadatos, elija 2.

  Para obtener más información, consulte Detalles avanzados.

Old console

Para exigir el uso de IMDSv2 en una nueva instancia

- Al iniciar una nueva instancia en la consola de Amazon EC2, seleccione las siguientes opciones en la página Configure Instance Details (Configurar detalles de instancia):
  - En Advanced Details (Detalles avanzados), en Metadata accessible (Metadatos accesibles), seleccione Enabled (Habilitado).
  - En Metadata version (Versión de metadatos), seleccione V2 (token required) (V2 (token obligatorio)).

Para obtener más información, consulte Paso 3: Configurar los detalles de la instancia.

AWS CLI

Para exigir el uso de IMDSv2 en una nueva instancia

En el siguiente ejemplo de run-instances, se inicia una instancia `c6i.large` con `--metadata-options` establecido en `HttpTokens=required`. Cuando se especifica un valor para `HttpTokens`, también se debe establecer `HttpEndpoint` en `enabled`. Debido a que el encabezado del token de seguridad está establecido en `required` para las solicitudes de recuperación de metadatos, se requiere que la instancia use IMDSv2 al solicitar los metadatos de la instancia.

En un entorno de contenedores, cuando se requiere IMDSv2, recomendamos establecer el límite de saltos en 2 con `HttpPutResponseHopLimit=2`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c6i.large \
 ...
    --metadata-options
 "HttpEndpoint=enabled,HttpTokens=required,HttpPutResponseHopLimit=2"
```

PowerShell

Para exigir el uso de IMDSv2 en una nueva instancia

En el siguiente ejemplo del cmdlet New-EC2Instance, se inicia una instancia `c6i.large` con `MetadataOptions_HttpEndpoint` establecido en `enabled` y el parámetro `MetadataOptions_HttpTokens` en `required`. Cuando se especifica un valor para `HttpTokens`, también se debe establecer `HttpEndpoint` en `enabled`. Debido a que el encabezado del token de seguridad está establecido en `required` para las solicitudes de recuperación de metadatos, se requiere que la instancia use IMDSv2 al solicitar los metadatos de la instancia.

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType c6i.large `
    -MetadataOptions_HttpEndpoint enabled `
    -MetadataOptions_HttpTokens required
```

AWS CloudFormation

Para especificar las opciones de metadatos de una instancia con AWS CloudFormation, consulte la propiedad AWS::EC2::LaunchTemplate MetadataOptions en la Guía del usuario de AWS CloudFormation.

Configuración de la AMI

Al registrar una AMI nueva o modificar una AMI existente, puede establecer el parámetro `imds-support` en `v2.0`. Las instancias iniciadas desde esta AMI tendrán el valor de Metadata version (Versión de metadatos) establecido en V2 only (token required) (Solo V2 [token obligatorio]) (consola) o `HttpTokens` establecido en `required` (AWS CLI). Con esta configuración, la instancia requiere que se utilice IMDSv2 al solicitar los metadatos de la instancia.

Tenga en cuenta que cuando establezca `imds-support` en `v2.0`, las instancias iniciadas desde esta AMI también tendrán Metadata response hop limit (Límite de saltos de respuesta de metadatos) (consola) o `http-put-response-hop-limit` (AWS CLI) establecido en 2.

> **Important**
>
> No utilice este parámetro a menos que el software de AMI sea compatible con IMDSv2. Después de establecer el valor en `v2.0`, no podrá deshacer el cambio. La única forma de "restablecer" la AMI es crear una AMI nueva a partir de la instantánea subyacente.

Para configurar una nueva AMI para IMDSv2

Utilice uno de los siguientes métodos para configurar una nueva AMI de IMDSv2.

AWS CLI

El siguiente ejemplo de register-image registra una AMI mediante la instantánea especificada de un volumen raíz de EBS como dispositivo `/dev/xvda`. Especifique `v2.0` para el parámetro `imds-support` a fin de que las instancias que se lancen desde esta AMI requieran que se utilice IMDSv2 al solicitar metadatos de instancia.

```
aws ec2 register-image \
    --name my-image \
    --root-device-name /dev/xvda \
    --block-device-mappings DeviceName=/dev/
xvda,Ebs={SnapshotId=snap-0123456789example} \
    --architecture x86_64 \
    --imds-support v2.0
```

PowerShell

En el siguiente ejemplo del cmdlet Register-EC2Image, se registra una AMI mediante la instantánea especificada de un volumen raíz de EBS como dispositivo `/dev/xvda`. Especifique `v2.0` para el parámetro `ImdsSupport` a fin de que las instancias que se lancen desde esta AMI requieran que se utilice IMDSv2 al solicitar metadatos de instancia.

```
Import-Module AWS.Tools.EC2  # Required for Amazon.EC2.Model object creation.
Register-EC2Image `
    -Name 'my-image' `
    -RootDeviceName /dev/xvda `
    -BlockDeviceMapping  (
    New-Object `
        -TypeName Amazon.EC2.Model.BlockDeviceMapping `
        -Property @{
        DeviceName = '/dev/xvda';
        EBS        = (New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice -Property
 @{
                SnapshotId = 'snap-0123456789example';
                VolumeType = 'gp3'
                } )
        }  ) `
    -Architecture X86_64 `
    -ImdsSupport v2.0
```

Para configurar una AMI existente para IMDSv2

Utilice uno de los métodos siguientes para configurar una AMI existente para IMDSv2.

AWS CLI

El siguiente ejemplo modify-image-attribute modifica una AMI existente únicamente para IMDSv2. Especifique `v2.0` para el parámetro `imds-support` a fin de que las instancias que se lancen desde esta AMI requieran que se utilice IMDSv2 al solicitar metadatos de instancia.

```
aws ec2 modify-image-attribute \
    --image-id ami-0123456789example \
    --imds-support v2.0
```

PowerShell

En el siguiente ejemplo de cmdlet Edit-EC2ImageAttribute, se modifica una AMI existente únicamente para IMDSv2. Especifique `v2.0` para el parámetro `imds-support` a fin de que las instancias que se lancen desde esta AMI requieran que se utilice IMDSv2 al solicitar metadatos de instancia.

```
Edit-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -ImdsSupport 'v2.0'
```

Uso de una política de IAM

También puede crear una política de IAM que impida a los usuarios iniciar nuevas instancias a menos que exijan el uso de IMDSv2 en la nueva instancia.

Para exigir el uso de IMDSv2 en todas las instancias nuevas mediante una política de IAM

Para asegurarse de que los usuarios solo puedan iniciar instancias que exigen el uso de IMDSv2 al solicitar metadatos de instancia, puede especificar que la condición para exigir IMDSv2 debe cumplirse antes de iniciar una instancia. Para ver una política de IAM de ejemplo, consulte Trabajar con metadatos de instancias.

Habilitación de los puntos de conexión IPv4 e IPv6 de IMDS

El IMDS tiene dos puntos de conexión en una instancia: IPv4 (`169.254.169.254`) e IPv6 (`[fd00:ec2::254]`). Al habilitar el IMDS, el punto de conexión IPv4 se habilita automáticamente. El punto de conexión IPv6 permanece deshabilitado incluso si se lanza una instancia en una subred de solo IPv6. Para habilitar el punto de conexión IPv6, tiene que hacerlo de manera explícita. Si habilita el punto de conexión IPv6, el punto de conexión IPv4 permanece habilitado.

Puede habilitar el punto de conexión IPv6 al momento de lanzar una instancia o después.

Requisitos para la habilitación de un punto de conexión IPv6

- El tipo de instancia seleccionado está basado en AWS Nitro System.
- Las subredes seleccionadas son compatibles con IPv6, y cada subred es de doble pila o solo IPv6.

Utilice uno de los siguientes métodos para lanzar una instancia con el punto de conexión IPv6 de IMDS habilitado.

New console

Para habilitar el punto de conexión IPv6 de IMDS en el momento del lanzamiento de una instancia

- Lance la instancia en la consola de Amazon EC2 con la siguiente información especificada en Advanced details (Detalles avanzados):
  - Para el punto de conexión IPv6 para la obtención de metadatos, seleccione Activado.

Para obtener más información, consulte Detalles avanzados.

AWS CLI

Para habilitar el punto de conexión IPv6 de IMDS en el momento del lanzamiento de una instancia

El siguiente ejemplo de run-instances inicia una instancia `c6i.large` con el punto de conexión de IPv6 habilitado para IMDS. Para habilitar el punto de conexión de IPv6, para el parámetro `--metadata-options`, especifique `HttpProtocolIpv6=enabled`. Cuando se especifica un valor para `HttpProtocolIpv6`, también se debe establecer `HttpEndpoint` en `enabled`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c6i.large \
    ...
    --metadata-options "HttpEndpoint=enabled,HttpProtocolIpv6=enabled"
```

PowerShell

Para habilitar el punto de conexión IPv6 de IMDS en el momento del lanzamiento de una instancia

En el siguiente ejemplo del cmdlet New-EC2Instance, se inicia una instancia `c6i.large` con el punto de conexión de IPv6 habilitado para IMDS. Para habilitar el punto de conexión IPv6, especifique `MetadataOptions_HttpProtocolIpv6` como `enabled`. Cuando se especifica un valor para `MetadataOptions_HttpProtocolIpv6`, también se debe establecer `MetadataOptions_HttpEndpoint` en `enabled`.

```
New-EC2Instance `
```

```
    -ImageId ami-0abcdef1234567890 `
    -InstanceType c6i.large `
    -MetadataOptions_HttpEndpoint enabled `
    -MetadataOptions_HttpProtocolIpv6 enabled
```

Desactivar el acceso a los metadatos de instancia

Puede desactivar el acceso a los metadatos de la instancia si deshabilita el IMDS al iniciar una instancia. Puede activar el acceso más adelante si vuelve a habilitar el IMDS. Para obtener más información, consulte Activación del acceso a los metadatos de instancias.

Important

Puede optar por deshabilitar el IMDS durante la inicialización o después. Si deshabilita el IMDS durante la inicialización, es posible que lo siguiente no funcione:

- Es posible que no tenga acceso mediante SSH a su instancia. `public-keys/0/openssh-key`, que es la clave de SSH pública de su instancia, no estará accesible porque normalmente se proporciona y se accede a ella desde los metadatos de la instancia de EC2.
- Los datos de usuario de EC2 no estarán disponibles y no se ejecutarán al iniciar la instancia. Los datos de usuario de EC2 se alojan en el IMDS. Si deshabilita el IMDS, desactiva de forma eficaz el acceso a los datos de los usuarios.

Para acceder a esta funcionalidad, puede volver a habilitar el IMDS después de la inicialización.

New console

Para desactivar el acceso a los metadatos de instancia durante la inicialización

- Lance la instancia en la consola de Amazon EC2 con la siguiente información especificada en Advanced details (Detalles avanzados):
  - Para Metadatos accesibles, elija Disabled (Deshabilitado).

Para obtener más información, consulte Detalles avanzados.

Old console

Para desactivar el acceso a los metadatos de instancia durante la inicialización

- Lance la instancia en la consola de Amazon EC2 con la siguiente opción seleccionada en la página Configure Instance Details (Configurar detalles de la instancia):
  - En Advanced Details (Detalles avanzados), en Metadata accessible (Metadatos accesibles), seleccione Disabled (Desactivado).

Para obtener más información, consulte Paso 3: Configurar los detalles de la instancia.

AWS CLI

Para desactivar el acceso a los metadatos de instancia durante la inicialización

Lance la instancia con `--metadata-options` establecido en `HttpEndpoint=disabled`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c6i.large \
    ...
    --metadata-options "HttpEndpoint=disabled"
```

PowerShell

Para desactivar el acceso a los metadatos de instancia durante la inicialización

En el siguiente ejemplo del cmdlet New-EC2Instance, se inicia una instancia con `MetadataOptions_HttpEndpoint` establecido en `disabled`.

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType c6i.large `
    -MetadataOptions_HttpEndpoint disabled
```

AWS CloudFormation

Para especificar las opciones de metadatos de una instancia con AWS CloudFormation, consulte la propiedad AWS::EC2::LaunchTemplate MetadataOptions en la Guía del usuario de AWS CloudFormation.

Configurar las opciones de metadatos para instancias existentes

Puede modificar las opciones de metadatos para las instancias existentes.

Además, puede crear una política de IAM que impida a los usuarios modificar las opciones de metadatos de instancias existentes. Para controlar qué usuarios pueden modificar las opciones de metadatos de instancias, especifique una política que impida a todos los usuarios que no tengan un rol determinado utilizar la API ModifyInstanceMetadataOptions. Para ver una política de IAM de ejemplo, consulte Trabajar con metadatos de instancias.

Opciones de metadatos de instancia de consulta para instancias existentes

Puede consultar las opciones de metadatos de las instancias existentes mediante uno de los siguientes métodos.

Console

Consulta de las opciones de metadatos de una instancia existente mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Seleccione la instancia.
4. Elija Acciones, Configuración de la instancia y Modificar opciones de metadatos de instancia.
5. Revise las opciones de metadatos de la instancia actuales en el cuadro de diálogo Modificar las opciones de metadatos de la instancia.

AWS CLI

Para consultar las opciones de metadatos de una instancia existente mediante el AWS CLI

Utilice el comando de la CLI describe-instances.

```
aws ec2 describe-instances \
    --instance-id i-1234567898abcdef0 \
    --query 'Reservations[].Instances[].MetadataOptions'
```

PowerShell

Para consultar las opciones de metadatos de una instancia existente mediante las herramientas para PowerShell

Utilice el cmdlet Get-EC2Instance.

```
(Get-EC2Instance `
    -InstanceId i-1234567898abcdef0).Instances.MetadataOptions
```

Requerir el uso de IMDSv2

Utilice uno de los siguientes métodos para modificar las opciones de metadatos de una instancia existente para requerir que se utilice IMDSv2 al requerir los metadatos de instancia. Cuando se requiere IMDSv2, no se puede usar IMDSv1.

> **Note**
>
> Antes de solicitar el uso de IMDSv2, asegúrese de que la instancia no esté realizando llamadas a IMDSv1. La métrica `MetadataNoToken` de CloudWatch rastrea las llamadas de IMDSv1. Cuando `MetadataNoToken` no registra ningún uso de IMDSv1 en una instancia, la instancia estará lista para requerir IMDSv2.

Console

Para exigir el uso de IMDSv2 en una instancia existente

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Seleccione la instancia.
4. Elija Acciones, Configuración de la instancia y Modificar opciones de metadatos de instancia.
5. En el cuadro de diálogo Modificar opciones de metadatos de instancia, haga lo siguiente:
   a. En Servicio de metadatos de instancia, seleccione Habilitar.
   b. En IMDSv2, seleccione Obligatorio.
   c. Seleccione Guardar.

AWS CLI

Para exigir el uso de IMDSv2 en una instancia existente

Use el comando de la CLI modify-instance-metadata-options y establezca el parámetro `http-tokens` en `required`. Cuando se especifica un valor para `http-tokens`, también se debe establecer `http-endpoint` en `enabled`.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567898abcdef0 \
    --http-tokens required \
    --http-endpoint enabled
```

PowerShell

Para exigir el uso de IMDSv2 en una instancia existente

Utilice el cmdlet Edit-EC2InstanceMetadataOption y defina el parámetro `HttpTokens` en `required`. Cuando se especifica un valor para `HttpTokens`, también se debe establecer `HttpEndpoint` en `enabled`.

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567898abcdef0 `
    -HttpTokens required `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Restauración del uso de IMDSv1

Cuando se requiera IMDSv2, IMDSv1 no funcionará al solicitar metadatos de instancia. Cuando IMDSv2 sea opcional, tanto IMDSv2 como IMDSv1 funcionarán. Por lo tanto, para reemplazar IMDSv1, haga que IMDSv2 sea opcional mediante alguno de los métodos siguientes.

Console

Para restaurar el uso de IMDSv1 en una instancia

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Seleccione la instancia.
4. Elija Acciones, Configuración de la instancia y Modificar opciones de metadatos de instancia.
5. En el cuadro de diálogo Modificar opciones de metadatos de instancia, haga lo siguiente:

a. Para Servicio de metadatos de instancia, asegúrese de que esté seleccionada la opción Habilitar.

b. En IMDSv2, seleccione Opcional.

c. Seleccione Guardar.

AWS CLI

Para restaurar el uso de IMDSv1 en una instancia

Puede utilizar el comando de la CLI modify-instance-metadata-options `http-tokens` establecido en `optional` para restaurar el uso de IMDSv1 cuando se solicitan metadatos de la instancia.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567898abcdef0 \
    --http-tokens optional \
    --http-endpoint enabled
```

PowerShell

Para restaurar el uso de IMDSv1 en una instancia

Puede usar el cmdlet Edit-EC2InstanceMetadataOption con `HttpTokens` establecido en `optional`, para restaurar el uso de IMDSv1 al solicitar los metadatos de la instancia.

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567898abcdef0 `
    -HttpTokens optional `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Cambio del límite de saltos de respuesta PUT

En las instancias existentes, puede modificar la configuración del límite de saltos de respuesta PUT.

Actualmente, solo la AWS CLI y los AWS SDK admiten cambiar el límite de saltos de respuesta PUT.

AWS CLI

Para cambiar el límite de saltos de respuesta PUT

Use el comando de la CLI modify-instance-metadata-options y establezca el parámetro `http-put-response-hop-limit` en el número de saltos necesario. En el siguiente ejemplo, el límite de saltos se ha establecido en `3`. Tenga en cuenta que al especificar un valor para `http-put-response-hop-limit`, también debe establecer `http-endpoint` en `enabled`.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567898abcdef0 \
    --http-put-response-hop-limit 3 \
    --http-endpoint enabled
```

PowerShell

Para cambiar el límite de saltos de respuesta PUT

Utilice el cmdlet Edit-EC2InstanceMetadataOption y defina el parámetro `HttpPutResponseHopLimit` para el número de saltos obligatorio. En el siguiente ejemplo, el límite de saltos se ha establecido en `3`. Tenga en cuenta que al especificar un valor para `HttpPutResponseHopLimit`, también debe establecer `HttpEndpoint` en `enabled`.

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567898abcdef0 `
    -HttpPutResponseHopLimit 3 `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Habilitación de los puntos de conexión IPv4 e IPv6 de IMDS

El IMDS tiene dos puntos de conexión en una instancia: IPv4 (`169.254.169.254`) e IPv6 (`[fd00:ec2::254]`). Al habilitar el IMDS, el punto de conexión IPv4 se habilita automáticamente. El punto de conexión IPv6 permanece deshabilitado incluso si se lanza una instancia en una subred de solo IPv6. Para habilitar el punto de conexión IPv6, tiene que hacerlo de manera explícita. Si habilita el punto de conexión IPv6, el punto de conexión IPv4 permanece habilitado.

Puede habilitar el punto de conexión IPv6 al momento de lanzar una instancia o después.

Requisitos para la habilitación de un punto de conexión IPv6

- El tipo de instancia seleccionado está basado en AWS Nitro System.
- Las subredes seleccionadas son compatibles con IPv6, y cada subred es de doble pila o solo IPv6.

En la actualidad, solo la AWS CLI y los AWS SDK son compatibles con la habilitación de un punto de conexión IPv6 de IMDS después del lanzamiento de una instancia.

AWS CLI

Para habilitar el punto de conexión IPv6 de IMDS para una instancia

Use el comando de la CLI modify-instance-metadata-options y establezca el parámetro `http-protocol-ipv6` en `enabled`. Tenga en cuenta que al especificar un valor para `http-protocol-ipv6`, también debe establecer `http-endpoint` en `enabled`.

```
aws ec2 modify-instance-metadata-options \
 --instance-id i-1234567898abcdef0 \
 --http-protocol-ipv6 enabled \
 --http-endpoint enabled
```

PowerShell

Para habilitar el punto de conexión IPv6 de IMDS para una instancia

Utilice el cmdlet Edit-EC2InstanceMetadataOption y defina el parámetro `HttpProtocolIpv6` en `enabled`. Tenga en cuenta que al especificar un valor para `HttpProtocolIpv6`, también debe establecer `HttpEndpoint` en `enabled`.

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567898abcdef0 `
    -HttpProtocolIpv6 enabled `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Activación del acceso a los metadatos de instancias

Puede activar el acceso a los metadatos de instancia al habilitar el punto de conexión HTTP del IMDS en la instancia, independientemente de la versión del IMDS que utilice. Para anular este cambio en cualquier momento, deshabilite el punto de conexión HTTP.

Utilice uno de los métodos siguientes para activar el acceso a los metadatos de una instancia en una instancia.

Console

Para activar el acceso a los metadatos de instancia

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Seleccione la instancia.
4. Elija Acciones, Configuración de la instancia y Modificar opciones de metadatos de instancia.
5. En el cuadro de diálogo Modificar opciones de metadatos de instancia, haga lo siguiente:
   a. En Servicio de metadatos de instancia, seleccione Habilitar.
   b. Seleccione Guardar.

AWS CLI

Para activar el acceso a los metadatos de instancia

Use el comando de la CLI modify-instance-metadata-options y establezca el parámetro `http-endpoint` en `enabled`.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567898abcdef0 \
    --http-endpoint enabled
```

PowerShell

Para activar el acceso a los metadatos de instancia

Utilice el cmdlet Edit-EC2InstanceMetadataOption y defina el parámetro `HttpEndpoint` en `enabled`.

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567898abcdef0 `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Desactivar el acceso a los metadatos de instancia

Puede desactivar el acceso a los metadatos de instancia al deshabilitar el punto de conexión HTTP del IMDS en la instancia, independientemente de la versión del IMDS que utilice. Puede anular este cambio en cualquier momento mediante la activación del punto de conexión HTTP.

Utilice uno de los métodos siguientes para desactivar el acceso a los metadatos de una instancia.

Console

Para desactivar el acceso a los metadatos de instancia

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Seleccione la instancia.
4. Elija Acciones, Configuración de la instancia y Modificar opciones de metadatos de instancia.
5. En el cuadro de diálogo Modificar opciones de metadatos de instancia, haga lo siguiente:
   a. Para Servicio de metadatos de instancia, desactive Habilitar.
   b. Seleccione Guardar.

AWS CLI

Para desactivar el acceso a los metadatos de instancia

Use el comando de la CLI modify-instance-metadata-options y establezca el parámetro `http-endpoint` en `disabled`.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567898abcdef0 \
    --http-endpoint disabled
```

PowerShell

Para desactivar el acceso a los metadatos de instancia

Utilice el cmdlet Edit-EC2InstanceMetadataOption y defina el parámetro `HttpEndpoint` en `disabled`.

```
(Edit-EC2InstanceMetadataOption `
```

```
    -InstanceId i-1234567898abcdef0 `
    -HttpEndpoint disabled).InstanceMetadataOptions
```

Recuperar metadatos de instancia

Puesto que los metadatos de la instancia se encuentran disponibles en la instancia en ejecución, no se necesita utilizar la consola de Amazon EC2 ni la AWS CLI. Esto puede resultar de utilidad al escribir scripts para ejecutarlos desde la instancia. Por ejemplo, puede obtener acceso a la dirección IP local de la instancia desde los metadatos de la instancia para administrar una conexión a una aplicación externa.

Los metadatos de instancia se dividen en categorías. Para obtener una descripción de cada categoría de metadatos de instancia, consulte Categorías de metadatos de instancia.

Para ver todas las categorías de metadatos de instancia dentro de una instancia en ejecución, utilice las siguientes URI IPv4 o IPv6.

IPv4

```
http://169.254.169.254/latest/meta-data/
```

IPv6

```
http://[fd00:ec2::254]/latest/meta-data/
```

Las direcciones IP son direcciones de enlace local y solo son válidas desde la instancia. Para obtener más información, consulte Direcciones de enlace local en esta guía de usuario y en Link-local address en Wikipedia.

> **Note**
>
> En los ejemplos de esta sección, se utiliza la dirección IPv4 de IMDS: `169.254.169.254`. Si recupera metadatos de instancia para las instancias de EC2 a través de la dirección IPv6, asegúrese de habilitar y utilizar la dirección IPv6 en su lugar: `[fd00:ec2::254]`. La dirección IPv6 de IMDS es compatible con los comandos de IMDSv2. Solo se puede acceder a la dirección IPv6 en instancias basadas en AWS Nitro System y en una subred compatible con IPv6 (de doble pila o solo IPv6).

El formato de comando difiere en función de si usa IMDSv1 o IMDSv2. De forma predeterminada, puede usar ambas versiones de IMDS. Para exigir el uso de IMDSv2, consulte Utilizar IMDSv2.

Para recuperar los metadatos de la instancia en instancias Linux

También puede usar una herramienta como cURL, tal como se muestra en el siguiente ejemplo.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/
```

Para recuperar los metadatos de la instancia en instancias Windows

Puede utilizar cmdlets de PowerShell para recuperar el URI. Por ejemplo, si ejecuta la versión 3.0 o posterior de PowerShell, debe utilizar el siguiente cmdlet.

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/
```

Si no quiere utilizar PowerShell, puede instalar una herramienta de terceros como GNU Wget o cURL.

> **Important**
>
> Si instala una herramienta de terceros en una instancia de Windows, asegúrese de leer detenidamente la documentación asociada, ya que el método para llamar al HTTP y el formato de salida pueden ser distintos a lo que se indica aquí.

Costos

No se le cobrará por las solicitudes HTTP utilizadas para recuperar metadatos de instancia y datos de usuario.

Consideraciones

Para evitar problemas con la recuperación de metadatos de instancia, tenga en cuenta lo siguiente:

- En un entorno de contenedores, recomendamos establecer el límite de saltos en 2.

  Los AWS SDK utilizan llamadas a IMDSv2 de forma predeterminada. Si la IMDSv2 llamada no recibe respuesta, el SDK reintenta la llamada y, si aún no tiene éxito, utiliza IMDSv1. Esto puede generar un retraso, especialmente en un entorno de contenedor. En un entorno de contenedor, si el límite de saltos es 1, no devuelve la IMDSv2 respuesta porque ir al contenedor se considera un salto de red adicional. Para evitar el proceso de retroceso IMDSv1 y el retraso resultante, en un entorno de contenedor recomendamos que establezca el límite de saltos en 2. Para obtener más información, consulte Configurar las opciones de metadatos de instancia.

- (Solo en Windows) Cree AMI personalizadas con Windows Sysprep.

  Para asegurarse de que el IMDS funcione cuando inicie una instancia desde una AMI de Windows personalizada, la AMI debe ser una imagen estandarizada creada con Windows Sysprep. De lo contrario, IMDS no funcionará. Para obtener más información, consulte Creación de una AMI con Windows Sysprep.

- En el caso de IMDSv2, debe utilizar **`/latest/api/token`** al recuperar el token.

  La emisión de solicitudes PUT a cualquier ruta específica de la versión, como, por ejemplo, `/2021-03-23/api/token`, dará lugar a que el servicio de metadatos devuelva errores 403 Forbidden (403 Prohibido). Este es el comportamiento deseado.

- Si se requiere IMDSv2, IMDSv1 no funciona.

Puede comprobar si se requiere IMDSv2 para una instancia de la siguiente manera: seleccione la instancia para ver sus detalles y compruebe el valor de IMDSv2. El valor es Obligatorio (solo se puede usar IMDSv2) u Opcional (se pueden utilizar IMDSv2 e IMDSv1).

Respuestas y mensajes de error

Todos los metadatos de instancia se devuelven como texto (tipo de contenido HTTP `text/plain`).

La solicitud de un recurso de metadato concreto devuelve el valor correspondiente, o bien un código de error HTTP `404 - Not Found` si no se encuentra disponible el recurso.

La solicitud de un recurso de metadato general (el URI acaba en /) devuelve una lista de recursos disponibles, o bien un código de error HTTP `404 - Not Found` si no existe dicho recurso. Los elementos de la lista aparecen en líneas separadas que acaban con saltos de línea (ASCII 10).

Para las solicitudes realizadas con Servicio de metadatos de instancia versión 2, pueden aparecer los siguientes códigos de error HTTP:

- `400 - Missing or Invalid Parameters` – la solicitud PUT no es válida.
- `401 - Unauthorized` – la solicitud `GET` usa un token no válido. La acción recomendada es generar un token nuevo.
- `403 - Forbidden`: la solicitud no está permitida o IMDS está desactivado.

Ejemplos de recuperación de metadatos de instancia

En los siguientes ejemplos se proporcionan comandos que puede utilizar en una instancia de Amazon EC2. El formato de comando difiere en las instancias de Linux y Windows.

Ejemplos

- Obtener las versiones disponibles de los metadatos de instancia
- Obtener los elementos de metadatos del nivel superior
- Cómo obtener los valores de los elementos de metadatos
- Obtener la lista de claves públicas disponibles
- Mostrar los formatos en los que se encuentra disponible la clave pública 0
- Obtener la clave pública 0 (en formato de clave OpenSSH)
- Obtener el ID de subred de una instancia

- Obtener las etiquetas de instancia de una instancia

Obtener las versiones disponibles de los metadatos de instancia

Este ejemplo obtiene las versiones disponibles de los metadatos de la instancia. Cada versión hace referencia a una compilación de metadatos de instancia correspondiente al momento en que se publicaron nuevas categorías de metadatos de instancia. No existe una correlación entre las versiones de compilación de metadatos de instancia y las versiones de la API de Amazon EC2. Tiene disponibles las versiones anteriores en caso de que tenga scripts que se basen en la estructura y la información presente en la versión anterior.

> **Note**
>
> Para no tener que actualizar el código cada vez que Amazon EC2 publique una nueva compilación de metadatos de instancia, se recomienda utilizar `latest` en la ruta, no el número de versión. Por ejemplo, utilice `latest` de la siguiente manera: `curl http://169.254.169.254/latest/meta-data/ami-id`

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
```

```
2016-04-19
...
latest
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
...
latest
```

Windows

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
```

```
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
...
latest
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
...
latest
```

Obtener los elementos de metadatos del nivel superior

Este ejemplo obtiene los elementos de metadatos del nivel superior. Para obtener más información sobre los elementos en la respuesta, consulte Categorías de metadatos de instancia.

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
events/
hostname
iam/
instance-action
instance-id
instance-life-cycle
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
events/
hostname
iam/
```

```
instance-action
instance-id
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
```

Windows

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
hostname
iam/
instance-action
instance-id
instance-life-cycle
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
```

```
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
hostname
iam/
instance-action
instance-id
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
```

Cómo obtener los valores de los elementos de metadatos

En estos ejemplos se obtienen los valores de algunos elementos de metadatos de nivel superior del ejemplo anterior. Las solicitudes IMDSv2 usan el token almacenado creado en el comando de ejemplo anterior, siempre y cuando no haya vencido.

Linux

IMDSv2

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/ami-id
ami-0abcdef1234567890
```

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/reservation-id
r-0efghijk987654321
```

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/local-hostname
ip-10-251-50-12.ec2.internal
```

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/public-hostname
ec2-203-0-113-25.compute-1.amazonaws.com
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/ami-id
ami-0abcdef1234567890
```

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/reservation-id
r-0efghijk987654321
```

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/local-hostname
ip-10-251-50-12.ec2.internal
```

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-hostname
ec2-203-0-113-25.compute-1.amazonaws.com
```

Windows

IMDSv2

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/ami-id
ami-0abcdef1234567890
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/reservation-id
r-0efghijk987654321
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/local-hostname
ip-10-251-50-12.ec2.internal
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/public-hostname
ec2-203-0-113-25.compute-1.amazonaws.com
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/ami-id
ami-0abcdef1234567890
```

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/reservation-
id
r-0efghijk987654321
```

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/local-
hostname
ip-10-251-50-12.ec2.internal
```

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-
hostname
ec2-203-0-113-25.compute-1.amazonaws.com
```

Obtener la lista de claves públicas disponibles

Este ejemplo obtiene la lista de las claves públicas disponibles.

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/public-keys/
0=my-public-key
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/
0=my-public-key
```

Windows

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/public-keys/
0=my-public-key
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-keys/ 0=my-public-key
```

Mostrar los formatos en los que se encuentra disponible la clave pública 0

Este ejemplo muestra los formatos en los que se encuentra disponible la clave pública 0.

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/public-keys/0/
openssh-key
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/0/
openssh-key
```

Windows

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
openssh-key
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
openssh-key
```

Obtener la clave pública 0 (en formato de clave OpenSSH)

Este ejemplo obtiene la clave pública 0 (en formato de clave OpenSSH).

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
ssh-rsa MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
ssh-rsa MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

Windows

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
ssh-rsa MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
ssh-rsa MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

Obtener el ID de subred de una instancia

Este ejemplo obtiene el ID de subred de una instancia.

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/network/interfaces/macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/network/interfaces/macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

Windows

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -Uri http://169.254.169.254/latest/meta-data/network/interfaces/macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/network/interfaces/macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

Obtener las etiquetas de instancia de una instancia

En los ejemplos siguientes, la instancia de ejemplo tiene etiquetas en metadatos de instancia habilitadas y las etiquetas de las instancias `Name=MyInstance` y `Environment=Dev`.

Este ejemplo obtiene todas las claves de etiqueta de instancia de una instancia.

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/tags/instance
Name
Environment
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/tags/instance
Name
Environment
```

En el siguiente ejemplo, se recibe el valor de la clave de `Name` que se obtuvo en el ejemplo anterior. La solicitud IMDSv2 utiliza el token almacenado creado en el comando de ejemplo anterior, siempre y cuando no haya vencido.

IMDSv2

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/tags/instance/Name
MyInstance
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/tags/instance/Name
MyInstance
```

Windows

IMDSv2

```
PS C:\> $token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds"
 = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/tags/instance
Name
Environment
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/tags/instance
Name
Environment
```

En el siguiente ejemplo, se recibe el valor de la clave de `Name` que se obtuvo en el ejemplo anterior. La solicitud IMDSv2 utiliza el token almacenado creado en el comando de ejemplo anterior, siempre y cuando no haya vencido.

IMDSv2

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/tags/instance/Name
MyInstance
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/tags/
instance/Name
MyInstance
```

Limitación de consultas

Limitamos las consultas a IMDS por cada instancia y aplicamos límites en el número de conexiones simultáneas desde una instancia a IMDS.

Si utiliza IMDS para recuperar credenciales de seguridad de AWS, evite consultar credenciales en cada transacción o mientras se ejecuta una gran cantidad de procesos o subprocesos, ya que puede producirse una limitación controlada en las operaciones. En lugar de ello, se recomienda guardar en caché las credenciales hasta que comience a aproximarse su caducidad. Para obtener más información sobre el rol de IAM y las credenciales de seguridad asociadas al rol, consulte Recuperar credenciales de seguridad de los metadatos de la instancia.

Si experimenta limitaciones controladas al acceder a IMDS, vuelva a realizar la consulta con una estrategia de retroceso exponencial.

Limitación del acceso a IMDS

Puede plantearse el uso de reglas de firewall locales para desactivar el acceso de algunos o todos los procesos a IMDS.

> **Note**
>
> En el caso de las instancias integradas en el AWS Nitro System, se puede acceder a IMDS desde su propia red cuando un dispositivo de red de la VPC, como un enrutador virtual, reenvía paquetes a la dirección de IMDS y la comprobación de origen o destino predeterminada en la instancia se encuentra deshabilitada. Para evitar que un origen externo a la VPC llegue a IMDS, se recomienda modificar la configuración del dispositivo de red para eliminar los paquetes con la dirección IPv4 de destino de IMDS `169.254.169.254` y, si habilita el punto de conexión IPv6, la dirección IPv6 de IMDS `[fd00:ec2::254]`.

Linux

Uso de iptables para limitar el acceso

En el siguiente ejemplo se usan iptables de Linux y su módulo `owner` para impedir que el webserver Apache (basado en el ID de usuario de instalación predeterminado de `apache`) acceda a 169.254.169.254. Usa una regla de rechazo para rechazar todas las solicitudes de metadatos de instancia (IMDSv1 o IMDSv2) de cualquier proceso que se ejecute con ese usuario.

```
$ sudo iptables --append OUTPUT --proto tcp --destination 169.254.169.254 --match owner
 --uid-owner apache --jump REJECT
```

O, puede plantearse solo dar acceso a usuarios o grupos determinados, mediante el uso de reglas de permiso. Las reglas de permiso pueden ser más sencillas de administrar desde el punto de

vista de la seguridad, ya que requieren que tome una decisión acerca del software que necesita acceso a los metadatos de instancia. Si usa reglas de permiso, es menos probable que permita al software de forma involuntaria acceder al servicio de metadatos (al que no pretendía dar acceso) si posteriormente cambia el software o la configuración en una instancia. También puede combinar el uso de grupos con reglas de permiso, de manera que pueda añadir y eliminar usuarios de un grupo permitido sin tener que cambiar la regla del firewall.

En el siguiente ejemplo se impide el acceso a IMDS a todos los procesos, excepto a aquellos que se ejecutan en la cuenta de usuario `trustworthy-user`.

```
$ sudo iptables --append OUTPUT --proto tcp --destination 169.254.169.254 --match
 owner ! --uid-owner trustworthy-user --jump REJECT
```

> **Note**
>
> - Para usar reglas de firewall locales, debe adaptar los comandos de ejemplo anteriores para adaptarlos a sus necesidades.
> - De forma predeterminada, las reglas iptables no persisten en los reinicios de sistema. Pueden convertirse en persistentes con el uso de funcionalidades del SO, que no se describen aquí.
> - El módulo `owner` de iptables solo coincide con la pertenencia a grupos si el grupo es el grupo principal de un usuario local determinado. Los otros grupos no coinciden.

Uso de PF o IPFW para limitar el acceso

Si usa FreeBSD u OpenBSD, también puede plantearse usar PF o IPFW. En los siguientes ejemplos se limita el acceso a IMDS a únicamente el usuario raíz.

PF

```
$ block out inet proto tcp from any to 169.254.169.254
```

```
$ pass out inet proto tcp from any to 169.254.169.254 user root
```

IPFW

```
$ allow tcp from any to 169.254.169.254 uid root
```

```
$ deny tcp from any to 169.254.169.254
```

> **Note**
>
> El orden de los comandos PF e IPFW importa. El valor predeterminado de PF es la última regla coincidente y el de IPFW es la primera regla coincidente.

Windows

Uso del firewall de Windows para limitar el acceso

El ejemplo de PowerShell utiliza el firewall integrado de Windows para impedir que el webserver Apache (basado en el ID de usuario de instalación predeterminado de `NT AUTHORITY\IUSR`) acceda a 169.254.169.254. Usa una regla de rechazo para rechazar todas las solicitudes de metadatos de instancia (IMDSv1 o IMDSv2) de cualquier proceso que se ejecute con ese usuario.

```
PS C:\> $blockPrincipal = New-Object -TypeName System.Security.Principal.NTAccount ("NT
 AUTHORITY\IUSR")
PS C:\> $BlockPrincipalSID =
 $blockPrincipal.Translate([System.Security.Principal.SecurityIdentifier]).Value
PS C:\> $BlockPrincipalSDDL = "D:(A;;CC;;;$BlockPrincipalSID)"
PS C:\> New-NetFirewallRule -DisplayName "Block metadata service from IIS" -Action
 block -Direction out `
-Protocol TCP -RemoteAddress 169.254.169.254 -LocalUser $BlockPrincipalSDDL
```

O, puede plantearse solo dar acceso a usuarios o grupos determinados, mediante el uso de reglas de permiso. Las reglas de permiso pueden ser más sencillas de administrar desde el punto de vista de la seguridad, ya que requieren que tome una decisión acerca del software que necesita acceso a los metadatos de instancia. Si usa reglas de permiso, es menos probable que permita al software de forma involuntaria acceder al servicio de metadatos (al que no pretendía dar acceso) si posteriormente cambia el software o la configuración en una instancia. También puede combinar el uso de grupos con reglas de permiso, de manera que pueda añadir y eliminar usuarios de un grupo permitido sin tener que cambiar la regla del firewall.

El siguiente ejemplo impide acceder a los metadatos de instancia a todos los procesos que se ejecutan como grupo de SO especificado en la variable `blockPrincipal` (en este ejemplo, el

grupo Windows `Everyone`), excepto para los procesos especificados en `exceptionPrincipal` (en este ejemplo, un grupo denominado `trustworthy-users`). Debe especificar los dos principios de rechazo y de permiso porque el firewall de Windows, a diferencia de la regla `! --uid-owner trustworthy-user` en iptables de Linux, no proporciona un mecanismo abreviado para permitir solo un principal determinado (usuario o grupo) mediante el rechazo de los demás.

```
PS C:\> $blockPrincipal = New-Object -TypeName System.Security.Principal.NTAccount
 ("Everyone")
PS C:\> $BlockPrincipalSID =
 $blockPrincipal.Translate([System.Security.Principal.SecurityIdentifier]).Value
PS C:\> $exceptionPrincipal = New-Object -TypeName System.Security.Principal.NTAccount
 ("trustworthy-users")
PS C:\> $ExceptionPrincipalSID =
 $exceptionPrincipal.Translate([System.Security.Principal.SecurityIdentifier]).Value
PS C:\> $PrincipalSDDL = "O:LSD:(D;;CC;;;$ExceptionPrincipalSID)(A;;CC;;;
$BlockPrincipalSID)"
PS C:\> New-NetFirewallRule -DisplayName "Block metadata service for
 $($blockPrincipal.Value), exception: $($exceptionPrincipal.Value)" -Action block -
Direction out `
-Protocol TCP -RemoteAddress 169.254.169.254 -LocalUser $PrincipalSDDL
```

> **Note**
>
> Para usar reglas de firewall locales, debe adaptar los comandos de ejemplo anteriores para adaptarlos a sus necesidades.

Uso de las reglas netsh para limitar el acceso

Puede plantearse bloquear todo el software con reglas `netsh` pero son menos flexibles.

```
C:\> netsh advfirewall firewall add rule name="Block metadata service altogether"
 dir=out protocol=TCP remoteip=169.254.169.254 action=block
```

> **Note**
>
> - Para usar reglas de firewall locales, debe adaptar los comandos de ejemplo anteriores para adaptarlos a sus necesidades.

- Las reglas `netsh` deben establecerse a partir de un símbolo del sistema elevado y no pueden fijarse para denegar o permitir determinados principales.

Trabajar con los datos de usuario de la instancia

Puede usar los datos de usuario de la instancia para personalizar las instancias. Cuando inicia una instancia, puede almacenar parámetros o scripts como datos de usuario. Todos los scripts de los datos de usuario se ejecutan al iniciar la instancia. Puede ver los datos de usuario como un atributo de la instancia. También puede ver los datos de usuario de su instancia a través del servicio de metadatos de instancias (IMDS).

Consideraciones

- Los datos de usuario se tratan como datos opacos: lo que facilita es lo que obtiene. La instancia es quien debe interpretarlos.
- Los datos de usuario deben estar codificados con base64. La consola de Amazon EC2 puede realizar la codificación con base64 por usted, o bien puede aceptar la entrada codificada con base64.
- Los datos de usuario están limitados a 16 KB, sin formato, antes de cifrarlo en base64. El tamaño de una cadena de longitud n tras el cifrado en base64 es ceil(n/3)*4.
- Los datos de usuario deben descodificarse en base64 al recuperarlos. Los datos se descodifican automáticamente si los recupera con los metadatos de instancia o la consola.
- Si detiene una instancia, modifica sus datos de usuario y la inicia de nuevo, los datos de usuario actualizados no se ejecutan automáticamente al iniciar la instancia. Con instancias de Windows, puede configurar los ajustes para que los scripts de datos de usuario actualizados se ejecuten una vez al iniciar la instancia, o bien cada vez que esta se inicie o se reinicie.
- Los datos de usuario son un atributo de la instancia. Si crea una AMI a partir de una instancia, los datos de usuario de la instancia no se incluyen en la AMI.

Especificar los datos de usuario de la instancia durante la inicialización

Puede especificar los datos de usuario al iniciar una instancia. Para obtener instrucciones sobre la consola, consulte Especificar los datos de usuario de la instancia durante la inicialización. Para ver un ejemplo de Linux en el que se usa la AWS CLI, consulte the section called “Datos de usuario y

las AWS CLI". Para ver un ejemplo de Windows en el que se utiliza Tools for Windows PowerShell, consulte the section called "Datos de usuario y las Tools for Windows PowerShell".

Modificar los datos de usuario de la instancia

Puede modificar los datos de usuario de las instancias con un volumen raíz de EBS. La instancia debe estar detenida. Para obtener instrucciones sobre la consola, consulte Visualizar y actualizar los datos de usuario de la instancia. Para ver un ejemplo de Linux en el que se usa la AWS CLI, consulte modify-instance-attribute. Para ver un ejemplo de Windows en el que se utiliza Tools for Windows PowerShell, consulte the section called "Datos de usuario y las Tools for Windows PowerShell".

Recuperación de los datos de usuario de la instancia desde su instancia

> **Note**
>
> En los ejemplos de esta sección, se utiliza la dirección IPv4 de IMDS: `169.254.169.254`. Si recupera metadatos de instancia para las instancias de EC2 a través de la dirección IPv6, asegúrese de habilitar y utilizar la dirección IPv6 en su lugar: `[fd00:ec2::254]`. La dirección IPv6 de IMDS es compatible con los comandos de IMDSv2. Solo se puede acceder a la dirección IPv6 en instancias basadas en AWS Nitro System y en una subred compatible con IPv6 (de doble pila o solo IPv6).

Para recuperar datos de usuario de una instancia, utilice el siguiente URI.

```
http://169.254.169.254/latest/user-data
```

Las solicitudes de datos de usuario devuelven los datos tal cual (tipo de contenido `application/octet-stream`). Si la instancia no tiene ningún dato de usuario, la solicitud devuelve `404 - Not Found`.

Este ejemplo devuelve datos de usuario que se proporcionaron como texto separado por comas.

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
```

```
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/user-
data
1234,john,reboot,true | 4512,richard, | 173,,,
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

Windows

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

IMDSv1

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = Invoke-RestMethod
 -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} `
-Method PUT -Uri http://169.254.169.254/latest/api/token} -Method GET -uri
 http://169.254.169.254/latest/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

Este ejemplo devuelve datos de usuario que se proporcionaron como script.

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/user-
data
#!/bin/bash
yum update -y
```

```
service httpd start
chkconfig httpd on
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/user-data
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

Windows

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/user-data
<powershell>
$file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/user-data
<powershell>
$file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

Recuperación de los datos de usuario de la instancia desde su equipo

Puede recuperar datos de usuario de una instancia desde su propio equipo. Para obtener instrucciones sobre la consola, consulte Visualizar y actualizar los datos de usuario de la instancia.

Para ver un ejemplo en el que se usa la AWS CLI, consulte Datos de usuario y las AWS CLI. Para ver un ejemplo en el que se utiliza Tools for Windows PowerShell, consulte Datos de usuario y las Tools for Windows PowerShell.

Recuperar datos dinámicos

Para recuperar datos dinámicos de una instancia en ejecución, utilice el siguiente URI.

```
http://169.254.169.254/latest/dynamic/
```

> **Note**
>
> En los ejemplos de esta sección, se utiliza la dirección IPv4 de IMDS: `169.254.169.254`. Si recupera metadatos de instancia para las instancias de EC2 a través de la dirección IPv6, asegúrese de habilitar y utilizar la dirección IPv6 en su lugar: `[fd00:ec2::254]`. La dirección IPv6 de IMDS es compatible con los comandos de IMDSv2. Solo se puede acceder a la dirección IPv6 en instancias basadas en AWS Nitro System y en una subred compatible con IPv6 (de doble pila o solo IPv6).

En este ejemplo se muestra cómo recuperar categorías de identidad de instancia de alto nivel.

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/dynamic/instance-identity/
rsa2048
pkcs7
document
signature
dsa2048
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/dynamic/instance-identity/
rsa2048
pkcs7
```

```
document
signature
dsa2048
```

Windows

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/dynamic/instance-identity/
document
rsa2048
pkcs7
signature
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/dynamic/instance-identity/
document
rsa2048
pkcs7
signature
```

Para obtener más información sobre datos dinámicos y ejemplos de cómo recuperarlos, consulte Documentos de identidad de instancias.

Categorías de metadatos de instancia

Los metadatos de instancia se dividen en categorías. Para recuperar los metadatos de instancia, debe especificar la categoría en la solicitud, y los metadatos se devolverán en la respuesta.

Cuando se publican nuevas categorías, se crea una nueva compilación de metadatos de instancia con un nuevo número de versión. En la siguiente tabla, la columna Version when category was released (Versión cuando se publicó la categoría) especifica la versión de la compilación correspondiente al momento cuando se publicó una categoría de metadatos de instancia. Para

no tener que actualizar el código cada vez que Amazon EC2 publique una nueva compilación de metadatos de instancia, utilice `latest` en lugar del número de versión en las solicitudes de metadatos. Para obtener más información, consulte Obtener las versiones disponibles de los metadatos de instancia.

Cuando Amazon EC2 publica una nueva categoría de metadatos de instancia, es posible que los metadatos de instancia de la nueva categoría no estén disponibles para las instancias existentes. Con las instancias creadas en el sistema Nitro, se pueden recuperar los metadatos de la instancia únicamente para aquellas categorías que estaban disponibles en el momento de la inicialización. Para instancias con el hipervisor Xen, se puede detener y luego iniciar la instancia para actualizar las categorías que están disponibles para ella.

En la siguiente tabla se enumeran las categorías de los metadatos de instancia. Algunos de los nombres de categoría son marcadores de posición para datos que son exclusivos de su instancia. Por ejemplo, *`mac`* representa la dirección MAC de la interfaz de red. Debe sustituir los marcadores de posición por valores reales en el momento de recuperar los metadatos de la instancia.

Categoría	Descripción	Versión cuando se publicó la categoría
`ami-id`	El ID de la AMI utilizada para iniciar la instancia.	1.0
`ami-launch-index`	Si inicia varias instancias con la misma llamada a `RunInstances`, este valor indica el orden de inicialización de cada instancia. El valor de la primera instancia iniciada es 0. Si inicia instancias con una flota de EC2 o Auto Scaling, este valor siempre es 0.	1.0
`ami-manifest-path`	La ruta al archivo de manifiesto de AMI en Amazon S3. Si ha utilizado una AMI respaldada por Amazon EBS para iniciar la instancia, el resultado devuelto es `unknown`.	1.0

Categoría	Descripción	Versión cuando se publicó la categoría
`ancestor-ami-ids`	Los ID de AMI de cualquier instancia que se haya vuelto a agrupar para crear esta AMI. Este valor solo existirá si el archivo de manifiesto de AMI contenía una clave `ancestor-amis` .	10-10-2007
`autoscaling/target-lifecycle-state`	Valor que muestra el estado de ciclo de vida de Auto Scaling de destino al que va a pasar una instancia de Auto Scaling. Presente cuando la instancia pasa a uno de los estados de ciclo de vida de destino después del 10 de marzo de 2022. Valores posibles: `Detached` | `InService` | `Standby` | `Terminated` | `Warmed:Hibernated` | `Warmed:Running` | `Warmed:Stopped` | `Warmed:Terminated` . Consulte Recuperar el estado de ciclo de vida de destino a través de los metadatos de instancia en la Guía del usuario de Amazon EC2 Auto Scaling.	15/07/2021
`block-device-mapping/ami`	El dispositivo virtual que contiene el sistema de archivos raíz o de arranque.	15-12-2007

Categoría	Descripción	Versión cuando se publicó la categoría
`block-device-mapping/ebs` N	Los dispositivos virtuales asociados a cualquier volumen de Amazon EBS. Los volúmenes de Amazon EBS solo están disponibles en los metadatos si se encontraban presentes en el momento de la inicialización o la última vez que se inició la instancia . La N indica el índice del volumen de Amazon EBS (como `ebs1` o `ebs2`).	15-12-2007

Categoría	Descripción	Versión cuando se publicó la categoría
`block-device-mapping/ephemeral` N	Los dispositivos virtuales de los volúmenes de almacenes de instancias que no son de NVMe. La N indica el índice de cada volumen. Es posible que el número de volúmenes del almacén de instancias en la asignación del dispositivo de bloque no coincida con el número real de volúmenes del almacén de instancias para la instancia. El tipo de instancia determina el número de volúmenes del almacén de instancias que están disponibles para una instancia. Si el número de volúmenes de almacén de instancias en una asignación de dispositivo de bloque excede el número disponible para una instancia, los volúmenes de almacén de instancias adicionales se ignoran.	15-12-2007
`block-device-mapping/root`	Son los dispositivos o las particiones virtuales asociados a los dispositivos raíz o las particiones en el dispositivo virtual, donde el sistema de archivos raíz (/ o C:) se asocia a la instancia concreta.	15-12-2007
`block-device-mapping/swap`	Los dispositivos virtuales asociados a `swap`. No siempre están presentes.	15-12-2007

Categoría	Descripción	Versión cuando se publicó la categoría
`elastic-gpus/associations/` *`elastic-gpu-id`*	Si la instancia tiene una GPU elástica adjunta a la instancia, contiene una cadena JSON con información sobre la GPU elástica, incluida información de ID y de conexión.	30/11/2016
`elastic-inference/associations/` *`eia-id`*	Si hay un acelerador de Elastic Inference asociado a la instancia , contiene una cadena JSON con información sobre el acelerador de Elastic Inference, incluido su ID y tipo.	29-11-2018
`events/maintenance/history`	Si hay eventos de mantenimiento completados o cancelados para la instancia, contiene una cadena JSON con información sobre los eventos. Si desea obtener más información, consulte el apartado Para ver el historial de los eventos completados o cancelados.	17/08/2018
`events/maintenance/scheduled`	Si hay eventos de mantenimiento activos para la instancia, contiene una cadena JSON con información sobre los eventos. Para obtener más información, consulte Ver eventos programados.	17/08/2018

Categoría	Descripción	Versión cuando se publicó la categoría
`events/recommendations/rebalance`	Tiempo aproximado, en UTC, en el que se emite la notificación de recomendación de reequilibrio de la instancia de EC2 para la instancia. A continuación, se muestra un ejemplo de los metadatos de esta categoría: `{"noticeTime": "2020-11-05T08:22:00Z"}` . Esta categoría sólo está disponible luego de emitir la notificación. Para obtener más información, consulte Recomendación de reequilibrio de instancias de EC2.	27/10/2020
`hostname`	Si la instancia de EC2 utiliza la asignación de nombre basada en IP (IPBN), este es el nombre de host de DNS IPv4 privado de la instancia. Si la instancia de EC2 utiliza asignación de nombre basada en recursos (RBN), este es el RBN. En los casos en los que existen varias interfaces de red, esto se refiere al dispositivo eth0 (el dispositivo cuyo número de dispositivo es 0). Para obtener más información sobre IPBN y RBN, consulte Tipos de nombres de host de instancias de Amazon EC2.	1.0

Categoría	Descripción	Versión cuando se publicó la categoría
`iam/info`	Si existe un rol de IAM asociado a la instancia, contiene información acerca de la última vez que se actualizó el perfil de instancia, incluida la fecha de LastUpdated de la instancia, InstanceProfileArn e InstanceProfileId. De lo contrario, no está presente.	12-01-2012
`iam/security-credentials/role-name`	Si hay un rol de IAM asociado a la instancia, *`role-name`* es el nombre del rol y *`role-name`* contiene las credenciales de seguridad temporales asociadas al rol (para obtener más información, consulte Recuperar credenciales de seguridad de los metadatos de la instancia). De lo contrario, no está presente.	12-01-2012
`identity-credentials/ec2/info`	Información sobre las credenciales en `identity-credentials/ec2/security-credentials/ec2-instance` .	23/05/2018

Categoría	Descripción	Versión cuando se publicó la categoría
`identity-credentials/ec2/security-credentials/ec2-instance`	Credenciales del rol de identidad de instancia que permiten que el software de la instancia se identifique como AWS para admitir características como la conexión de instancias de EC2 y la configuración de administración de host predeterminada de AWS Systems Manager. Estas credenciales no tienen políticas adjuntas, por lo que no tienen permisos de API de AWS adicionales más allá de identificar la instancia en la característica de AWS. Para obtener más información, consulte Roles de identidad de instancia.	23/05/2018
`instance-action`	Notifica a la instancia que debe reiniciarse como preparación para la agrupación. Valores válidos: `none` | `shutdown` | `bundle-pending` .	01-09-2008
`instance-id`	El ID de esta instancia.	1.0
`instance-life-cycle`	La opción de compra de esta instancia. Para obtener más información, consulte Opciones de compra de instancias.	01-10-2019
`instance-type`	El tipo de instancia. Para obtener más información, consulte Tipos de instancias de Amazon EC2.	29-08-2007

Categoría	Descripción	Versión cuando se publicó la categoría
`ipv6`	La dirección IPv6 de la instancia . En los casos en los que existen varias interfaces de red, esto se refiere a la interfaz de red del dispositivo eth0 (el dispositivo cuyo número de dispositivo es 0) y la primera IPv6 asignada. Si no existe ninguna dirección IPv6 en la interfaz de red [0], este elemento no está configurado y da como resultado una respuesta HTTP 404.	03/01/2021
`kernel-id`	El ID del kernel iniciado con esta instancia, si se aplica.	01-02-2008
`local-hostname`	En los casos en los que existen varias interfaces de red, esto se refiere al dispositivo eth0 (el dispositivo cuyo número de dispositivo es 0). Si la instancia de EC2 utiliza la asignación de nombre basada en IP (IPBN), este es el nombre de host de DNS IPv4 privado de la instancia . Si la instancia de EC2 utiliza asignación de nombre basada en recursos (RBN), este es el RBN. Para obtener más información acerca de la nomenclatura de IPBN, RBN e instancias de EC2, consulte Tipos de nombres de host de instancias de Amazon EC2.	19-01-2007

Categoría	Descripción	Versión cuando se publicó la categoría
`local-ipv4`	La dirección IPv4 privada de la instancia. En los casos en los que existen varias interfaces de red, esto se refiere al dispositivo eth0 (el dispositivo cuyo número de dispositivo es 0). Si se trata de una instancia de solo IPv6, este elemento no está configurado y da como resultado una respuesta HTTP 404.	1.0
`mac`	La dirección de control de acceso de medios (MAC) de la instancia . En los casos en los que existen varias interfaces de red, esto se refiere al dispositivo eth0 (el dispositivo cuyo número de dispositivo es 0).	01-01-2011
`metrics/vhostmd`	Ya no está disponible.	01/05/2011
`network/interfaces/ macs/mac/device-number`	El número exclusivo de dispositivo asociado a esa interfaz. El número de dispositivo se corresponde con el nombre del dispositivo; por ejemplo, un `device-number` de 2 es para el dispositivo eth2. Esta categoría se corresponde con los campos `DeviceIndex` y `device-index` que utilizan la API de Amazon EC2 y los comandos de EC2 para AWS CLI.	01-01-2011

Categoría	Descripción	Versión cuando se publicó la categoría
`network/interfaces/macs/mac/interface-id`	El ID de la interfaz de red.	01-01-2011
`network/interfaces/macs/mac/ipv4-associations/public-ip`	Las direcciones IPv4 privadas asociadas a cada dirección IP pública y que están asignadas a esa interfaz.	01-01-2011
`network/interfaces/macs/mac/ipv6s`	Las direcciones IPv6 asignadas a la interfaz.	30-06-2016
`network/interfaces/macs/mac/ipv6-prefix`	Los prefijos de IPv6 asignados a la interfaz de red.	
`network/interfaces/macs/mac/local-hostname`	El nombre de host DNS IPv4 privado de la instancia. En los casos en los que existen varias interfaces de red, esto se refiere al dispositivo eth0 (el dispositivo cuyo número de dispositivo es 0). Si se trata de una instancia de solo IPv6, este es el nombre basado en recursos. Para obtener más información sobre IPBN y RBN, consulte Tipos de nombres de host de instancias de Amazon EC2.	19-01-2007
`network/interfaces/macs/mac/local-ipv4s`	Las direcciones IPv4 privadas asociadas a la interfaz. Si se trata de una interfaz de red de solo IPv6, este elemento no está configurado y da como resultado una respuesta HTTP 404.	01-01-2011

Categoría	Descripción	Versión cuando se publicó la categoría
`network/interfaces/macs/mac/mac`	La dirección MAC de la instancia.	01-01-2011
`network/interfaces/macs/`*`mac`*`/network-card`	El índice de la tarjeta de red. Algunos tipos de instancia admiten varias tarjetas de red.	2020-11-01
`network/interfaces/macs/mac/owner-id`	El ID del propietario de la interfaz de red. En entornos con varias interfaces, un tercero puede adjuntar una interfaz, como Elastic Load Balancing. El tráfico en una interfaz se factura siempre al propietario de la interfaz.	01-01-2011
`network/interfaces/macs/mac/public-hostname`	El DNS (IPv4) público de la interfaz. Esta categoría solo se devuelve si el atributo `enableDnsHostnames` está establecido en `true`. Para obtener más información, consulte Atributos de DNS para su VPC en la Guía del usuario de Amazon VPC. Si la instancia solo tiene una dirección IPv6 pública y ninguna dirección IPv4 pública, este elemento no está configurado y da como resultado una respuesta HTTP 404.	01-01-2011
`network/interfaces/macs/mac/public-ipv4s`	Direcciones IP públicas o direcciones IP elásticas asociadas a la interfaz. Puede haber varias direcciones IPv4 en una instancia.	01-01-2011

Categoría	Descripción	Versión cuando se publicó la categoría
`network/interfaces/macs/mac/security-groups`	Grupos de seguridad a los que pertenece la interfaz de red.	01-01-2011
`network/interfaces/macs/mac/security-group-ids`	Los ID de los grupos de seguridad a los que pertenece la interfaz de red.	01-01-2011
`network/interfaces/macs/mac/subnet-id`	El ID de la subred en la que reside la interfaz.	01-01-2011
`network/interfaces/macs/mac/subnet-ipv4-cidr-block`	El bloque de CIDR IPv4 de la subred en la que reside la interfaz.	01-01-2011
`network/interfaces/macs/mac/subnet-ipv6-cidr-blocks`	El bloque de CIDR IPv6 de la subred en la que reside la interfaz.	30-06-2016
`network/interfaces/macs/mac/vpc-id`	El ID de la VPC en la que reside la interfaz.	01-01-2011
`network/interfaces/macs/mac/vpc-ipv4-cidr-block`	El bloque de CIDR IPv4 principal de la VPC.	01-01-2011
`network/interfaces/macs/mac/vpc-ipv4-cidr-blocks`	bloques de CIDR IPv4 secundarios para la VPC.	30-06-2016
`network/interfaces/macs/mac/vpc-ipv6-cidr-blocks`	El bloque de CIDR IPv6 de la VPC en la que reside la interfaz.	30-06-2016
`placement/availability-zone`	La zona de disponibilidad en la que se ha iniciado la instancia.	01-02-2008

Categoría	Descripción	Versión cuando se publicó la categoría
`placement/availability-zone-id`	El ID de zona de disponibilidad estática en el que se inicia la instancia. El ID de zona de disponibilidad es coherente en todas las cuentas. Sin embargo, puede ser diferente de la zona de disponibilidad, que puede variar según la cuenta.	01-10-2019
`placement/group-name`	El nombre del grupo de ubicación en el que se inicia la instancia.	24/08/2020
`placement/host-id`	El ID del host en el que se inicia la instancia. Aplicable solo a hosts dedicados.	24/08/2020
`placement/partition-number`	El número de la partición en la que se inicia la instancia.	24/08/2020
`placement/region`	La región de AWS en la que se inicia la instancia.	24/08/2020
`product-codes`	Códigos de producto de AWS Marketplace asociados a la instancia, si existen.	01-03-2007

Categoría	Descripción	Versión cuando se publicó la categoría
`public-hostname`	El DNS público de la instancia (IPv4). Esta categoría solo se devuelve si el atributo `enableDnsHostnames` está establecido en `true`. Para obtener más información, consulte Atributos de DNS para su VPC en la Guía del usuario de Amazon VPC. Si la instancia solo tiene una dirección IPv6 pública y ninguna dirección IPv4 pública, este elemento no está configurado y da como resultado una respuesta HTTP 404.	19-01-2007
`public-ipv4`	La dirección IPv4 pública. Si se asocia una dirección IP elástica a la instancia, el valor devuelto es dicha dirección.	19-01-2007
`public-keys/0/openssh-key`	Clave pública. Solo se encuentra disponible si se facilita en el momento de la inicialización de la instancia.	1.0
`ramdisk-id`	El ID del disco RAM especificado en el momento de la inicialización, si se aplica.	10-10-2007
`reservation-id`	El ID de la reserva.	1.0

Categoría	Descripción	Versión cuando se publicó la categoría
`security-groups`	Los nombres de los grupos de seguridad aplicados a la instancia. Tras la inicialización, puede cambiar los grupos de seguridad de las instancias. Dichos cambios se reflejan aquí y en network/interfaces/macs/*mac*/security-groups.	1.0
`services/domain`	Es el dominio para los recursos de AWS de la región.	25-02-2014
`services/partition`	Partición en la que se encuentra el recurso. Para las regiones estándar de AWS, la partición es `aws`. Si tiene recursos en otras particiones, la partición es `aws-`*`partitionname`* . Por ejemplo, la partición de los recursos de la región China (Pekín) es `aws-cn`.	20-10-2015
`spot/instance-action`	La acción (hibernar, detener o terminar) y la hora aproximada, en UTC, a la que se producirá la acción. Este elemento está presente solo si se ha marcado la instancia de spot para hibernar, detener o terminar. Para obtener más información, consulte instance-action.	15/11/2016

Categoría	Descripción	Versión cuando se publicó la categoría
`spot/termination-time`	La hora aproximada, en UTC, a la que el sistema operativo de la instancia de spot recibirá la señal de apagado. Este elemento está presente y contiene un valor temporal (por ejemplo, 2015-01-05T18:02:00Z) solo si la instancia de spot se ha marcado para que Amazon EC2 la termine. El elemento termination-time no se establece en un horario si usted mismo ha terminado la instancia de spot. Para obtener más información, consulte termination-time.	05-11-2014
`tags/instance`	Las etiquetas de instancia asociadas a la instancia. Solo disponible si permite el acceso explícito a etiquetas en metadatos de instancia. Para obtener más información, consulte Permitir acceso a etiquetas en metadatos de instancia.	23/03/2021

Categorías de datos dinámicos

En la siguiente tabla se enumeran las categorías de los datos dinámicos.

Categoría	Descripción	Versión cuando se publicó la categoría
`fws/instance-monitoring`	Valor que muestra si el cliente ha habilitado la monitorización detallada de un minuto en CloudWatch. Valores válidos: `enabled | disabled`	04-04-2009
`instance-identity/document`	JSON que contiene atributos de instancia, como ID de instancia, dirección IP privada, etc. Consulte Documentos de identidad de instancias.	04-04-2009
`instance-identity/pkcs7`	Se utiliza para verificar la autenticidad del documento y el contenido en comparación con la firma. Consulte Documentos de identidad de instancias.	04-04-2009
`instance-identity/signature`	Otras partes pueden utilizar los datos para verificar su origen y autenticidad. Consulte Documentos de identidad de instancias.	04-04-2009

Ejemplo de Linux: valor de índice de inicialización de AMI

En este ejemplo se demuestra cómo se pueden usar los datos de usuario y los metadatos de instancia para configurar las instancias de Linux.

> **Note**
>
> En los ejemplos de esta sección, se utiliza la dirección IPv4 de IMDS: `169.254.169.254`. Si recupera metadatos de instancia para las instancias de EC2 a través de la dirección IPv6, asegúrese de habilitar y utilizar la dirección IPv6 en su lugar: `[fd00:ec2::254]`. La dirección IPv6 de IMDS es compatible con los comandos de IMDSv2. Solo se puede acceder a la dirección IPv6 en instancias basadas en AWS Nitro System y en una subred compatible con IPv6 (de doble pila o solo IPv6).

Alice desea iniciar cuatro instancias de su AMI de base de datos favorita, de modo que la primera sea la instancia original y las tres restantes actúen como réplicas. Al iniciarlas, desea agregar datos de usuario acerca de la estrategia de replicación para cada réplica. Es consciente de que estos datos estarán disponibles para las cuatro instancias, por lo que debe estructurar los datos de usuario de modo que cada instancia pueda reconocer qué partes se aplican a cada una. Lo puede hacer con el valor de metadato de instancia `ami-launch-index`, que será exclusivo para cada instancia. Si ha iniciado más de una instancia al mismo tiempo, `ami-launch-index` indica el orden en el que se ha iniciado la instancia. El valor de la primera instancia iniciada es `0`.

Estos son los datos de usuario que ha creado Alice.

```
replicate-every=1min | replicate-every=5min | replicate-every=10min
```

Los datos de `replicate-every=1min` definen la configuración de la primera réplica, `replicate-every=5min` define la configuración de la segunda réplica y así sucesivamente. Alice decide facilitar estos datos como una cadena ASCII con un símbolo de barra vertical (`|`) que delimita los datos de las distintas instancias.

Alice inicia cuatro instancias con el comando run-instances y especifica los datos de usuario.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --count 4 \
    --instance-type t2.micro \
    --user-data "replicate-every=1min | replicate-every=5min | replicate-every=10min"
```

Una vez iniciadas, todas las instancias tienen una copia de los datos de usuario y los metadatos comunes se muestran aquí:

- ID de la AMI: ami-0abcdef1234567890
- ID de reserva: r-1234567890abcabc0
- Claves públicas: ninguna
- Nombre de grupo de seguridad: predeterminado
- Tipo de instancia: t2.micro

Sin embargo, cada instancia tiene ciertos metadatos exclusivos.

instancia 1

Metadatos	Valor
instance-id	i-1234567890abcdef0
ami-launch-index	0
public-hostname	ec2-203-0-113-25.compute-1.amazonaws.com
public-ipv4	67.202.51.223
local-hostname	ip-10-251-50-12.ec2.internal
local-ipv4	10.251.50.35

instancia 2

Metadatos	Valor
instance-id	i-0598c7d356eba48d7
ami-launch-index	1
public-hostname	ec2-67-202-51-224.compute-1.amazonaws.com
public-ipv4	67.202.51.224
local-hostname	ip-10-251-50-36.ec2.internal
local-ipv4	10.251.50.36

instancia 3

Metadatos	Valor
instance-id	i-0ee992212549ce0e7
ami-launch-index	2
public-hostname	ec2-67-202-51-225.compute-1.amazonaws.com

Metadatos	Valor
public-ipv4	67.202.51.225
local-hostname	ip-10-251-50-37.ec2.internal
local-ipv4	10.251.50.37

instancia 4

Metadatos	Valor
instance-id	i-1234567890abcdef0
ami-launch-index	3
public-hostname	ec2-67-202-51-226.compute-1.amazonaws.com
public-ipv4	67.202.51.226
local-hostname	ip-10-251-50-38.ec2.internal
local-ipv4	10.251.50.38

Alice puede utilizar el valor `ami-launch-index` para determinar la parte de los datos de usuario que se aplican a una instancia en concreto.

1. Se conecta a una de las instancias y recupera `ami-launch-index` de esa instancia para asegurarse de que es una de las réplicas:

   IMDSv2

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/meta-data/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/ami-launch-index
   2
   ```

   Para los siguientes pasos, las solicitudes de IMDSv2 usan el token almacenado del comando IMDSv2 precedente, siempre y cuando el token no haya caducado.

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/ami-launch-index
2
```

2. Guarda `ami-launch-index` como variable.

   IMDSv2

   ```
   [ec2-user ~]$ ami_launch_index=`curl -H "X-aws-ec2-metadata-token: $TOKEN"
    http://169.254.169.254/latest/meta-data/ami-launch-index`
   ```

   IMDSv1

   ```
   [ec2-user ~]$ ami_launch_index=`curl http://169.254.169.254/latest/meta-data/ami-
   launch-index`
   ```

3. Guarda los datos de usuario como variable.

   IMDSv2

   ```
   [ec2-user ~]$ user_data=`curl -H "X-aws-ec2-metadata-token: $TOKEN"
    http://169.254.169.254/latest/user-data`
   ```

   IMDSv1

   ```
   [ec2-user ~]$ user_data=`curl http://169.254.169.254/latest/user-data`
   ```

4. Por último, Alice utiliza el comando cut para extraer la parte de los datos de usuario que se aplican a esa instancia.

   IMDSv2

   ```
   [ec2-user ~]$ echo $user_data | cut -d"|" -f"$ami_launch_index"
   replicate-every=5min
   ```

   IMDSv1

   ```
   [ec2-user ~]$ echo $user_data | cut -d"|" -f"$ami_launch_index"
   replicate-every=5min
   ```

Documentos de identidad de instancias

Cada instancia que inicie tiene un Documentos de identidad de instancia que proporciona información sobre la propia instancia. Puede utilizar el Documentos de identidad de instancia para validar los atributos de la instancia.

El documento de identidad de la instancia se genera cuando la instancia se detiene e inicia, se reinicia o se inicia. El documento de identidad de la instancia se expone (en formato JSON de texto sin formato) a través del servicio de metadatos de instancia (IMDS). La dirección IPv4 `169.254.169.254` es una dirección de enlace local y solo es válida desde la instancia. Para obtener más información, consulte Dirección de enlace local en Wikipedia. La dirección IPv6 `[fd00:ec2::254]` es una dirección local única y solo es válida desde la instancia. Para obtener más información, consulte Dirección local única en Wikipedia.

> **Note**
>
> En los ejemplos de esta sección, se utiliza la dirección IPv4 de IMDS: `169.254.169.254`. Si recupera metadatos de instancia para las instancias de EC2 a través de la dirección IPv6, asegúrese de habilitar y utilizar la dirección IPv6 en su lugar: `[fd00:ec2::254]`. La dirección IPv6 de IMDS es compatible con los comandos de IMDSv2. Solo se puede acceder a la dirección IPv6 en instancias basadas en AWS Nitro System y en una subred compatible con IPv6 (de doble pila o solo IPv6).

Puede recuperar el Documentos de identidad de instancia de una instancia en ejecución en cualquier momento. El Documentos de identidad de instancia contiene la información siguiente:

Datos	Descripción
`accountId`	El ID de la cuenta de AWS que inició la instancia.
`architecture`	La arquitectura de la AMI utilizada para iniciar la instancia (i386 | x86_64 | arm64).
`availabilityZone`	La zona de disponibilidad en la que se ejecuta la instancia.
`billingProducts`	Los productos de facturación de la instancia.

Datos	Descripción
devpayProductCodes	Obsoleto.
imageId	El ID de la AMI utilizada para iniciar la instancia.
instanceId	El ID de la instancia.
instanceType	El tipo de instancia de la instancia.
kernelId	El ID del kernel asociado a la instancia, si corresponde.
marketplaceProductCodes	El código de producto de AWS Marketplace de la AMI utilizada para iniciar la instancia.
pendingTime	La fecha y la hora en que se lanzó la instancia.
privateIp	La dirección IPv4 privada de la instancia.
ramdiskId	El ID del disco RAM asociado con la instancia, si procede.
region	La región en la que se está ejecutando la instancia.
version	La versión del formato de archivoDocumentos de identidad de instancia.

Recuperar el Documentos de identidad de instancia de texto sin formato

Para recuperar el Documentos de identidad de instancia de texto sin formato

Conéctese a la instancia y ejecute el siguiente comando.

Linux

IMDSv2

```
$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/dynamic/
instance-identity/document
```

IMDSv1

```
$ curl http://169.254.169.254/latest/dynamic/instance-identity/document
```

Windows

IMDSv2

```
PS C:\> [string]$token = (Invoke-WebRequest -Method Put -Headers @{'X-aws-
ec2-metadata-token-ttl-seconds' = '21600'} http://169.254.169.254/latest/api/
token).Content
```

```
PS C:\> (Invoke-WebRequest -Headers @{'X-aws-ec2-metadata-token' = $Token}
 http://169.254.169.254/latest/dynamic/instance-identity/document).Content
```

IMDSv1

```
PS C:\> (Invoke-WebRequest http://169.254.169.254/latest/dynamic/instance-identity/
document).Content
```

A continuación, se muestra un ejemplo del resultado.

```
{
    "devpayProductCodes" : null,
    "marketplaceProductCodes" : [ "1abc2defghijklm3nopqrs4tu" ],
    "availabilityZone" : "us-west-2b",
    "privateIp" : "10.158.112.84",
    "version" : "2017-09-30",
    "instanceId" : "i-1234567890abcdef0",
    "billingProducts" : null,
    "instanceType" : "t2.micro",
    "accountId" : "123456789012",
    "imageId" : "ami-5fb8c835",
    "pendingTime" : "2016-11-19T16:32:11Z",
    "architecture" : "x86_64",
    "kernelId" : null,
    "ramdiskId" : null,
    "region" : "us-west-2"
}
```

Verificar la Documentos de identidad de instancia

Si tiene la intención de utilizar el contenido del Documentos de identidad de instancia para un propósito importante, debe verificar su contenido y autenticidad antes de usarlo.

El Documentos de identidad de instancia de texto sin formato se acompaña de tres firmas resumidas y cifradas. Puede utilizar estas firmas para verificar el origen y la autenticidad del Documentos de identidad de instancia y la información que incluye. Se proporcionan las siguientes firmas:

- Firma codificada en base64: este es un hash SHA256 codificado en base64 del Documentos de identidad de instancia cifrado mediante un par de claves RSA.
- Firma PKCS7: este es un hash SHA1 del Documentos de identidad de instancia cifrado mediante un par de claves DSA.
- Firma RSA-2048: este es un hash SHA256 del Documentos de identidad de instancia cifrado utilizando un par de claves RSA-2048.

Cada firma está disponible en un punto de conexión diferente en los metadatos de la instancia. Puede usar cualquiera de estas firmas dependiendo de sus requisitos de cifrado y hash. Para verificar las firmas, debe usar el correspondiente certificado público de AWS.

En los temas siguientes se proporcionan pasos detallados para validar el Documentos de identidad de instancia usando cada firma.

- Uso de la firma PKCS7 para verificar el Documentos de identidad de instancia
- Uso de la firma codificada en base64 para verificar el Documentos de identidad de instancia
- Uso de la firma RSA-2048 para verificar el Documentos de identidad de instancia

Uso de la firma PKCS7 para verificar el Documentos de identidad de instancia

En este tema, se explica cómo verificar el documento de identidad de la instancia mediante la firma PKCS7 y el certificado público DSA de AWS.

instancias de Linux

Para verificar el documento de identidad de la instancia mediante la firma PKCS7 y el certificado público DSA de AWS

1. Conéctese a la instancia.

2. Recupere la firma PKCS7 de los metadatos de la instancia y agréguela a un archivo nuevo denominado `pkcs7` junto con el encabezado y el pie de página requeridos. Utilice uno de los siguientes comandos dependiendo de la versión IMDS utilizada por la instancia.

   IMDSv2

   ```
   $ echo "-----BEGIN PKCS7-----" >> pkcs7 \
   && TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
   metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   dynamic/instance-identity/pkcs7 >> pkcs7 \
   && echo "" >> pkcs7 \
   && echo "-----END PKCS7-----" >> pkcs7
   ```

   IMDSv1

   ```
   $ echo "-----BEGIN PKCS7-----" >> pkcs7 \
   && curl -s http://169.254.169.254/latest/dynamic/instance-identity/pkcs7
    >> pkcs7 \
   && echo "" >> pkcs7 \
   && echo "-----END PKCS7-----" >> pkcs7
   ```

3. Busque el certificado público DSA para su región en Certificados públicos de AWS y agregue el contenido a un archivo nuevo denominado `certificate`.

4. Utilice el comando openSSL smime para verificar la firma. Incluya la opción `-verify` para indicar que es necesario verificar la firma, y la opción `-noverify` para indicar que no es necesario verificar el certificado.

   ```
   $ openssl smime -verify -in pkcs7 -inform PEM -certfile certificate -noverify | tee
    document
   ```

   Si la firma es válida, aparecerá el mensaje `Verification successful`.

   El comando también escribe el contenido del documento de identidad de la instancia en un nuevo archivo llamado `document`. Puede comparar el contenido del documento de identidad de la instancia de los metadatos de la instancia con el contenido de este archivo mediante los siguientes comandos.

   ```
   $ openssl dgst -sha256 < document
   ```

```
$ curl -s -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
dynamic/instance-identity/document | openssl dgst -sha256
```

Si no se puede verificar la firma, póngase en contacto con AWS Support.

instancias de Windows

Requisitos previos

Este procedimiento requiere la clase Microsoft .NET Core de `System.Security`. Para agregar la clase a la sesión de PowerShell, ejecute el siguiente comando.

```
PS C:\> Add-Type -AssemblyName System.Security
```

> **Note**
>
> El comando agrega la clase solo a la sesión actual de PowerShell. Si inicia una nueva sesión, debe ejecutar el comando de nuevo.

Para verificar el documento de identidad de la instancia mediante la firma PKCS7 y el certificado público DSA de AWS

1. Conéctese a la instancia.
2. Recupere la firma PKCS7 de los metadatos de instancia, conviértala en una matriz de bytes y agréguela a una variable denominada `$Signature`. Utilice uno de los siguientes comandos dependiendo de la versión IMDS utilizada por la instancia.

   IMDSv2

   ```
   PS C:\> [string]$token = (Invoke-WebRequest -Method Put -Headers @{'X-aws-
   ec2-metadata-token-ttl-seconds' = '21600'} http://169.254.169.254/latest/api/
   token).Content
   ```

   ```
   PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
   instance-identity/pkcs7).Content)
   ```

IMDSv1

```
PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest
 http://169.254.169.254/latest/dynamic/instance-identity/pkcs7).Content)
```

3. Recupere el documento de identidad de instancia de texto sin formato de los metadatos de instancia, conviértalo en una matriz de bytes y agréguelo a una variable denominada `$Document`. Utilice uno de los siguientes comandos dependiendo de la versión IMDS utilizada por la instancia.

   IMDSv2

   ```
   PS C:\> $Document = [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
   instance-identity/document).Content)
   ```

   IMDSv1

   ```
   PS C:\> $Document =  [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest
    http://169.254.169.254/latest/dynamic/instance-identity/document).Content)
   ```

4. Busque el certificado público DSA para su región en Certificados públicos de AWS y agregue el contenido a un archivo nuevo denominado `certificate.pem`.
5. Extraiga el certificado del archivo de certificado y guárdelo en una variable denominada `$Store`.

   ```
   PS C:\> $Store =
    [Security.Cryptography.X509Certificates.X509Certificate2Collection]::new([Security.Cryptog
   Path certificate.pem)))
   ```

6. Verifique la firma.

   ```
   PS C:\> $SignatureDocument = [Security.Cryptography.Pkcs.SignedCms]::new()
   ```

   ```
   PS C:\> $SignatureDocument.Decode($Signature)
   ```

   ```
   PS C:\> $SignatureDocument.CheckSignature($Store, $true)
   ```

Si la firma es válida, el comando no devuelve ningún resultado. Si no se puede verificar la firma, el comando devuelve `Exception calling "CheckSignature" with "2" argument(s): "Cannot find the original signer`. Si su firma no se puede verificar, póngase en contacto con AWS Support.

7. Valide el contenido del documento de identidad de instancia.

```
PS C:
\> [Linq.Enumerable]::SequenceEqual($SignatureDocument.ContentInfo.Content, $Document)
```

Si el contenido del documento de identidad de instancia es válido, el comando devuelve `True`. Si el documento de identidad de instancia no se puede validar, póngase en contacto con AWS Support.

Uso de la firma codificada en base64 para verificar el Documentos de identidad de instancia

En este tema, se explica cómo verificar el documento de identidad de la instancia mediante la firma codificada en base64 y el certificado público de RSA de AWS.

instancias de Linux

Para validar el documento de identidad de la instancia mediante la firma codificada en base64 y el certificado público del RSA de AWS

1. Conéctese a la instancia.
2. Recupere la firma codificada en base64 de los metadatos de la instancia, conviértala a binario y agréguela a un archivo denominado `signature`. Utilice uno de los siguientes comandos dependiendo de la versión IMDS utilizada por la instancia.

   IMDSv2

```
$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
dynamic/instance-identity/signature | base64 -d >> signature
```

IMDSv1

```
$ curl -s http://169.254.169.254/latest/dynamic/instance-identity/signature |
 base64 -d >> signature
```

3. Recupere el Documentos de identidad de instancia de texto sin formato de los metadatos de la instancia y agréguelo a un archivo denominado `document`. Utilice uno de los siguientes comandos dependiendo de la versión IMDS utilizada por la instancia.

   IMDSv2

   ```
   $ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
   metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   dynamic/instance-identity/document >> document
   ```

   IMDSv1

   ```
   $ curl -s http://169.254.169.254/latest/dynamic/instance-identity/document
    >> document
   ```

4. Busque el certificado público RSA para su región en Certificados públicos de AWS y agregue el contenido a un archivo nuevo denominado `certificate`.
5. Extraiga la clave pública del certificado público RSA de AWS y guárdela en un archivo denominado `key`.

   ```
   $ openssl x509 -pubkey -noout -in certificate >> key
   ```

6. Utilice el comando OpenSSL dgst para verificar el documento de identidad de instancia.

   ```
   $ openssl dgst -sha256 -verify key -signature signature document
   ```

   Si la firma es válida, aparecerá el mensaje `Verification successful`.

   El comando también escribe el contenido del documento de identidad de la instancia en un nuevo archivo llamado `document`. Puede comparar el contenido del documento de identidad de la instancia de los metadatos de la instancia con el contenido de este archivo mediante los siguientes comandos.

```
$ openssl dgst -sha256 < document
```

```
$ curl -s -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
dynamic/instance-identity/document | openssl dgst -sha256
```

Si no se puede verificar la firma, póngase en contacto con AWS Support.

instancias de Windows

Para validar el documento de identidad de la instancia mediante la firma codificada en base64 y el certificado público del RSA de AWS

1. Conéctese a la instancia.
2. Recupere la firma codificada en base64 de los metadatos de instancia, conviértala en una matriz de bytes y agréguela a la variable denominada `$Signature`. Utilice uno de los siguientes comandos dependiendo de la versión IMDS utilizada por la instancia.

   IMDSv2

   ```
   PS C:\> [string]$token = (Invoke-WebRequest -Method Put -Headers @{'X-aws-
   ec2-metadata-token-ttl-seconds' = '21600'} http://169.254.169.254/latest/api/
   token).Content
   ```

   ```
   PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
   instance-identity/signature).Content)
   ```

   IMDSv1

   ```
   PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest
    http://169.254.169.254/latest/dynamic/instance-identity/signature).Content)
   ```

3. Recupere el documento de identidad de instancia de texto sin formato de los metadatos de instancia, conviértalo en una matriz de bytes y agréguelo a una variable denominada `$Document`. Utilice uno de los siguientes comandos dependiendo de la versión IMDS utilizada por la instancia.

IMDSv2

```
PS C:\> $Document = [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest -Headers
 @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
instance-identity/document).Content)
```

IMDSv1

```
PS C:\> $Document =  [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest
 http://169.254.169.254/latest/dynamic/instance-identity/document).Content)
```

4. Busque el certificado público RSA para su región en Certificados públicos de AWS y agregue el contenido a un archivo nuevo denominado `certificate.pem`.
5. Verifique el documento de identidad de la instancia.

```
PS C:\> [Security.Cryptography.X509Certificates.X509Certificate2]::new((Resolve-
Path certificate.pem)).PublicKey.Key.VerifyData($Document, 'SHA256', $Signature)
```

Si la firma es válida, el comando devuelve `True`. Si no se puede verificar la firma, póngase en contacto con AWS Support.

Uso de la firma RSA-2048 para verificar el Documentos de identidad de instancia

En este tema, se explica cómo verificar el documento de identidad de la instancia mediante la firma RSA-2048 y el certificado público RSA-2048 de AWS.

instancias de Linux

Para verificar el documento de identidad de la instancia mediante la firma RSA-2048 y el certificado público RSA-2048 de AWS

1. Conéctese a la instancia.
2. Recupere la firma RSA-2048 de los metadatos de la instancia y agréguela a un archivo denominado `rsa2048` junto con el encabezado y el pie de página requeridos. Utilice uno de los siguientes comandos dependiendo de la versión IMDS utilizada por la instancia.

IMDSv2

```
$ echo "-----BEGIN PKCS7-----" >> rsa2048 \
&& TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
dynamic/instance-identity/rsa2048 >> rsa2048 \
&& echo "" >> rsa2048 \
&& echo "-----END PKCS7-----" >> rsa2048
```

IMDSv1

```
$ echo "-----BEGIN PKCS7-----" >> rsa2048 \
&& curl -s http://169.254.169.254/latest/dynamic/instance-identity/rsa2048
 >> rsa2048 \
&& echo "" >> rsa2048 \
&& echo "-----END PKCS7-----" >> rsa2048
```

3. Busque el certificado público RSA-2048 para su región en Certificados públicos de AWS y agregue el contenido a un archivo nuevo denominado `certificate`.
4. Utilice el comando openSSL smime para verificar la firma. Incluya la opción `-verify` para indicar que es necesario verificar la firma, y la opción `-noverify` para indicar que no es necesario verificar el certificado.

```
$ openssl smime -verify -in rsa2048 -inform PEM -certfile certificate -noverify |
 tee document
```

Si la firma es válida, aparecerá el mensaje `Verification successful`. Si no se puede verificar la firma, póngase en contacto con AWS Support.

instancias de Windows

Requisitos previos

Este procedimiento requiere la clase Microsoft .NET Core de `System.Security`. Para agregar la clase a la sesión de PowerShell, ejecute el siguiente comando.

```
PS C:\> Add-Type -AssemblyName System.Security
```

> **Note**
>
> El comando agrega la clase solo a la sesión actual de PowerShell. Si inicia una nueva sesión, debe ejecutar el comando de nuevo.

Para verificar el documento de identidad de la instancia mediante la firma RSA-2048 y el certificado público RSA-2048 de AWS

1. Conéctese a la instancia.
2. Recupere la firma RSA-2048 de los metadatos de instancia, conviértala en una matriz de bytes y agréguela a una variable denominada `$Signature`. Utilice uno de los siguientes comandos dependiendo de la versión IMDS utilizada por la instancia.

   IMDSv2

   ```
   PS C:\> [string]$token = (Invoke-WebRequest -Method Put -Headers @{'X-aws-
   ec2-metadata-token-ttl-seconds' = '21600'} http://169.254.169.254/latest/api/
   token).Content
   ```

   ```
   PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
   instance-identity/rsa2048).Content)
   ```

   IMDSv1

   ```
   PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest
    http://169.254.169.254/latest/dynamic/instance-identity/rsa2048).Content)
   ```

3. Recupere el documento de identidad de instancia de texto sin formato de los metadatos de instancia, conviértalo en una matriz de bytes y agréguelo a una variable denominada `$Document`. Utilice uno de los siguientes comandos dependiendo de la versión IMDS utilizada por la instancia.

   IMDSv2

   ```
   PS C:\> $Document = [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
   instance-identity/document).Content)
   ```

IMDSv1

```
PS C:\> $Document =  [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest
 http://169.254.169.254/latest/dynamic/instance-identity/document).Content)
```

4. Busque el certificado público RSA-2048 para su región en Certificados públicos de AWS y agregue el contenido a un archivo nuevo denominado `certificate.pem`.
5. Extraiga el certificado del archivo de certificado y guárdelo en una variable denominada `$Store`.

```
PS C:\> $Store =
 [Security.Cryptography.X509Certificates.X509Certificate2Collection]::new([Security.Cryptog
Path certificate.pem)))
```

6. Verifique la firma.

```
PS C:\> $SignatureDocument = [Security.Cryptography.Pkcs.SignedCms]::new()
```

```
PS C:\> $SignatureDocument.Decode($Signature)
```

```
PS C:\> $SignatureDocument.CheckSignature($Store, $true)
```

Si la firma es válida, el comando no devuelve ningún resultado. Si no se puede verificar la firma, el comando devuelve `Exception calling "CheckSignature" with "2" argument(s): "Cannot find the original signer`. Si su firma no se puede verificar, póngase en contacto con AWS Support.

7. Valide el contenido del documento de identidad de instancia.

```
PS C:
\> [Linq.Enumerable]::SequenceEqual($SignatureDocument.ContentInfo.Content, $Document)
```

Si el contenido del documento de identidad de instancia es válido, el comando devuelve `True`. Si el documento de identidad de instancia no se puede validar, póngase en contacto con AWS Support.

Certificados públicos de AWS

Los siguientes certificados públicos de AWS se pueden usar para verificar el contenido del documento de identidad de la instancia, tal como se describe en los siguientes temas:

- Verificar mediante la firma PKCS7
- Verificar mediante la firma codificada en base64
- Verificar mediante la firma RSA-2048

Asegúrese de usar el certificado correcto para su región y para el procedimiento de verificación que está usando. Si verifica la firma PKCS7, use el certificado DSA. Si verifica la firma codificada en base6, use el certificado RSA. Si verifica la firma RSA-2048, use el certificado RSA-2048.

Amplíe cada región a continuación para ver los certificados específicos de cada región.

Este de EE. UU. (Ohio): us-east-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
```

```
MIIDITCCAoqgAwIBAgIUVJTc+hOU+8Gk3JlqsX438Dk5c58wDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE3MTE0OVoXDTI5MDQyODE3MTE0OVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUVJTc+hOU
+8Gk3JlqsX438Dk5c58wEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAywJQaVNWJqW0R0T0xVOSoN1GLk9x9kKEuN67RN9CLin4dA97qa7Mr5W4P
FZ6vnh5CjOhQBRXV9xJUeYSdqVItNAUFK/fEzDdjf1nUfPlQ3OJ49u6CV01NoJ9m
usvY9kWcV46dqn2bk2MyfTTgvmeqP8fiMRPxxnVRkSzlldP5Fg==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAM07oeX4xevdMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNjA2MTAx
MjU4MThaGA8yMTk1MTExNDEyNTgxOFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA6v6kGMnRmFDLxBEqXzP4npnL65OO0kmQ7w8YXQygSdmNIoScGSU5wfh9
mZdcvCxCdxgALFsFqPvH8fqiE9ttI0fEfuZvHOs8wUsIdKr0Zz0MjSx3cik4tKET
ch0EKfMnzKOgDBavraCDeX1rUDU0Rg7HFqNAOry3uqDmnqtk00XC9GenS3z/7ebJ
fIBEPAam5oYMVFpX6M6St77WdNE8wEU8SuerQughiMVx9kMB07imeVHBiELbMQ0N
lwSWRL/61fA02keGSTfSp/0m3u+lesf2VwVFhqIJs+JbsEscPxOkIRlzy8mGd/JV
ONb/DQpTedzUKLgXbw7KtO3HTG9iXQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU2CTGYE5fTjx7gQXzdZSGPEWAJY4wgY4GA1UdIwSBhjCBg4AU2CTG
YE5fTjx7gQXzdZSGPEWAJY6hYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAM07oeX4xevdMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBANdqkIpVypr2PveqUsAKke1wKCOSuw1UmH9k
xX1/VRoHbrI/UznrXtPQOPMmHA2LKSTedwsJuorUn3cFH6qNs8ixBDrl8pZwfKOY
IBJcTFBbI1xBEFkZoO3wczzo5+8vPQ60RVqAaYb+iCa1HFJpccC3Ovajfa4GRdNb
n6FYnluIcDbmpcQePoVQwX7W3oOYLB1QLN7fE6H1j4TBIsFdO3OuKzmaifQlwLYt
DVxVCNDabpOr6Uozd5ASm4ihPPoEoKo7Ilp0fOT6fZ41U2xWA4+HF/89UoygZSo7
```

```
K+cQ90xGxJ+gmlYbLFR5rbJOLfjrgDAb2ogbFy8LzHo2ZtSe60M=
-----END CERTIFICATE-----
```

Este de EE. UU. (Virginia): us-east-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUE1y2NIKCU+Rg4uu4u32koG9QEYIwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE3MzQwMVoXDTI5MDQyODE3MzQwMVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUE1y2NIKC
```

```
U+Rg4uu4u32koG9QEYIwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAlxSmwcWnhT4uAeSinJuz+1BTcKhVSWb5jT8pYjQb8ZoZkXXRGb09mvYeU
NeqOBr27rvRAnaQ/9LUQf72+SahDFuS4CMI8nwowytqbmwquqFr4dxA/SDADyRiF
ea1UoMuNHTY49J/1vPomqsVn7mugTp+TbjqCfOJTpu0temHcFA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALFpzEAVWaQZMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
ODU5MTJaGA8yMTk1MDExNzA4NTkxMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAjS2vqZu9mEOhOq+0bRpAbCUiapbZMFNQqRg7kTlr7Cf+gDqXKpHPjsng
SfNz+JHQd8WPI+pmNs+q0Z2aTe23klmf2U52KH9/j1k8RlIbap/yFibFTSedmegX
E5r447GbJRsHUmuIIfZTZ/oRlpuIIO5/Vz7SOj22tdkdY2ADp7caZkNxhSP915fk
2jJMTBUOzyXUS2rBU/ulNHbTTeePjcEkvzVYPahD30TeQ+/A+uWUu89bHSQOJR8h
Um4cFApzZgN3aD5j2LrSMu2pctkQwf9CaWyVznqrsGYjYOY66LuFzSCXwqSnFBfv
fFBAFsjCgY24G2DoMyYkF3MyZlu+rwIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUrynSPp4uqSECwy+PiO4qyJ8TWSkwgY4GA1UdIwSBhjCBg4AUrynS
Pp4uqSECwy+PiO4qyJ8TWSmhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALFpzEAVWaQZMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBADW/s8lXijwdP6NkEoH1m9XLrvK4YTqkNfR6
er/uRRgTx2QjFcMNrx+g87gAml11z+D0crAZ5LbEhDMs+JtZYR3ty0HkDk6SJM85
haoJNAFF7EQ/zCp1EJRIkLLsC7bcDL/Eriv1swt78/BB4RnC9W9kSp/sxd5svJMg
N9a6FAplpNRsWAnbP8JBlAP93oJzblX2LQXgykTghMkQO7NaY5hg/H5o4dMPclTK
lYGqlFUCH6A2vdrxmpKDLmTn5//5pujdD2MN0df6sZWtxwZ0osljV4rDjm9Q3VpA
NWIsDEcp3GUB4proOR+C7PNkY+VGODitBOw09qBGosCBstwyEqY=
-----END CERTIFICATE-----
```

Oeste de EE. UU. (Norte de California): us-west-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
```

```
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUK2zmY9PUSTR7rc1k2OwPYu4+g7wwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE3MDI0M1oXDTI5MDQyODE3MDI0M1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUK2zmY9PU
STR7rc1k2OwPYu4+g7wwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQA1Ng4QmN4n7iPh5CnadSOc0ZfM7by0dBePwZJyGvOHdaw6P6E/vEk76KsC
Q8p+akuzVzVPkU4kBK/TRqLp19wEWoVwhhTaxHjQ1tTRHqXIVlrkw4JrtFbeNM21
GlkSLonuzmNZdivn9WuQYeGe7nUD4w3q9GgiF3CPorJe+UxtbA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJANNPkIpcyEtIMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEwMjkw
OTAzMDdaGA8yMTk1MDQwMzA5MDMwN1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
```

```
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEApHQGvHvq3SVCzDrC7575BW7GWLzcj8CLqYcL3YY7Jffupz7OjcftO57Z
4fo5Pj0CaS8DtPzh8+8vdwUSMbiJ6cDd3ooio3MnCq6DwzmsY+pY7CiI3UVG7KcH
4TriDqr1Iii7nB5MiPJ8wTeAqX89T3SYaf6Vo+4GCb3LCDGvnkZ9TrGcz2CHkJsj
AIGwgopFpwhIjVYm7obmuIxSIUv+oNH0wXgDL029Zd98SnIYQd/njiqkzE+lvXgk
4h4Tu17xZIKBgFcTtWPky+POGu81DYFqiWVEyR2JKKm2/iR1dL1YsT39kbNg47xY
aR129sS4nB5Vw3TRQA2jL0ToTIxzhQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUgepyiONs8j+q67dmcWu+mKKDa+gwgY4GA1UdIwSBhjCBg4AUgepy
iONs8j+q67dmcWu+mKKDa+ihYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJANNPkIpcyEtIMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAGLFWyutf1u0xcAc+kmnMPqtc/Q6b79VIX0E
tNoKMI2KR8lcV8ZElXDb0NC6v8UeLpe1WBKjaWQtEjL1ifKg9hdY9RJj4RXIDSK7
33qCQ8juF4vep2U5TTBd6hfWxt1Izi88xudjixmbpUU4YKr8UPbmixldYR+BEx0u
B1KJi9l1lxvuc/Igy/xeHOAZEjAXzVvHp8Bne33VVwMiMxWECZCiJxE4I7+Y6fqJ
pLLSFFJKbNaFyXlDiJ3kXyePEZSc1xiWeyRB2ZbTi5eu7vMG4i3AYWuFVLthaBgu
lPfHafJpj/JDcqt2vKUKfur5edQ6j1CGdxqqjawhOTEqcN8m7us=
-----END CERTIFICATE-----
```

Oeste de EE. UU. (Oregón): us-west-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUFx8PxCkbHwpD31bOyCtyz3GclbgwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE3MjM1OVoXDTI5MDQyODE3MjM1OVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUFx8PxCkb
HwpD31bOyCtyz3GclbgwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBzOl+9Xy1+UsbUBI95HO9mbbdnuX+aMJXgG9uFZNjgNEbMcvx+h8P9IMko
z7PzFdheQQ1NLjsHH9mSR1SyC4m9ja6BsejH5nLBWyCdjfdP3muZM4O5+r7vUa1O
dWU+hP/T7DUrPAIVMOE7mpYa+WPWJrN6BlRwQkKQ7twm9kDalA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALZL3lrQCSTMMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
OTAxMzJaGA8yMTk1MDExNzA5MDEzMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA02Y59qtAA0a6uzo7nEQcnJ26OKF+LRPwZfixBH+EbEN/Fx0gYy1jpjCP
s5+VRNg6/WbfqAsV6X2VSjUKN59ZMnMY9ALA/Ipz0n00Huxj38EBZmX/NdNqKm7C
qWu1q5kmIvYjKGiadfboU8wLwLcHo8ywvfgI6FiGGsEO9VMC56E/hL6Cohko11LW
dizyvRcvg/IidazVkJQCN/4zC9PUOVyKdhW33jXy8BTg/QH927QuNk+ZzD7HH//y
tIYxDhR6TIZsSnRjz3bOcEHxt1nsidc65mY0ejQty4hy7ioSiapw316mdbtE+RTN
fcH9FPIFKQNBpiqfAW5Ebp3Lal3/+wIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU7coQx8Qnd75qA9XotSWT3IhvJmowgY4GA1UdIwSBhjCBg4AU7coQ
x8Qnd75qA9XotSWT3IhvJmqhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALZL3lrQCSTMMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAFZ1e2MnzRaXCaLwEC1pW/f0oRG8nHrlPZ9W
OYZEWbh+QanRgaikBNDtVTwARQcZm3z+HWSkaIx3cyb6vM0DSkZuiwzm1LJ9rDPc
```

```
aBm03SEt5v8mcc7sXWvgFjCnUpzosmky6JheCD4O1Cf8k0olZ93FQnTrbg62OK0h
83mGCDeVKU3hLH97FYoUq+3N/IliWFDhvibAYYKFJydZLhIdlCiiB99AM6Sg53rm
oukS3csyUxZyTU2hQfdjyo1nqW9yhvFAKjnnggiwxNKTTPZzstKW8+cnYwiiTwJN
QpVoZdt0SfbuNnmwRUMi+QbuccXweav29QeQ3ADqjgB0CZdSRKk=
-----END CERTIFICATE-----
```

África (Ciudad del Cabo): af-south-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7DCCAqwCCQCncbCtQbjuyzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xOTA2MDQxMjQ4MDVaFw00
NTA2MDQxMjQ4MDVaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbYwggErBgcqhkjOOAQBMIIBHgKBgQC12Nr1gMrHcFSZ7S/A
pQBSCMHWmn2qeoQTMVWqe50fnTd0zGFxDdIjKxUK58/8zjWG5uR4TXRzmZpGpmXB
bSufAR6BGqud2LnT/HIWGJAsnX2uOtSyNfCoJigqwhea5w+CqZ6I7iBDdnB4TtTw
qO6TlnExHFVj8LMkylZgiaE1CQIVAIhdobse4K0QnbAhCL6R2euQzloXAoGAV/21
WUuMz/79Ga0JvQcz1FNy1sT0pU9rU4TenqLQIt5iccn/7EIfNtvVO5TZKulIKq7J
gXZr0x/KIT8zsNweetLOaGehPIYRMPX0vunMMR7hN7qA7W17WZv/76adywIsnDKq
ekfe15jinaX8MsKUdyDK7Y+ifCG4PVhoM4+W2XwDgYQAAoGAIxOKbVgwLxbn6Pi2
6hBOihFv16jKxAQI0hHzXJLV0Vyv9QwnqjJJRfOCy3dB0zicLXiIxeIdYfvqJr+u
hlN8rGxEZYYJjEUKMGvsc0DW85jonXz0bNfcP0aaKH0lKKVjL+OZi5n2kn9wgdo5
F3CVnMl8BUra8A1Tr2yrrE6TVZ4wCQYHKoZIzjgEAwMvADAsAhQfa7MCJZ+/TEY5
AUr0J4wm8VzjoAIUSYZVu2NdRJ/ERPmDfhW5EsjHlCA=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICNjCCAZ+gAwIBAgIJAKumfZiRrNvHMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTExMjcw
NzE0MDVaGA8yMTk5MDUwMjA3MTQwNVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQDFd571nUzVtke3rPyRkYfvs3jh0C0EMzzG72boyUNjnfw1+m0TeFraTLKb9T6F
7TuB/ZEN+vmlYqr2+5Va8U8qLbPF0bRH+FdaKjhgWZdYXxGzQzU3ioy5W5ZM1VyB
7iUsxEAlxsybC3ziPYaHI42UiTkQNahmoroNeqVyHNnBpQIDAQABMA0GCSqGSIb3
DQEBCwUAA4GBAAJLylWyElEgOpW4B1XPyRVD4pAds8Guw2+krgqkY0HxLCdjosuH
```

```
RytGDGN+q75aAoXzW5a7SGpxLxk6Hfv0xp3RjDHsoeP0i1d8MD3hAC5ezxS4oukK
s5gbPOnokhKTMPXbTdRn5ZifCbWlx+bYN/mTYKvxho7b5SVg2o1La9aK
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAIFI+O5A6/ZIMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTA2MDQx
MjQ4MDRaGA8yMTk4MTEwNzEyNDgwNFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAy7/WHBBHOrk+20aumT07g8rxrSM0UXgki3eYgKauPCG4Xx//vwQbuZwI
oeVmR9nqnhfij2wOcQdbLandh0EGtbxerete3IoXzd1KXJb11PVmzrzyu5SPBPuP
iCeV4qdjjkXo2YWM6t9YQ911hcG96YSp89TBXFYUh3KLxfqAdTVhuC0NRGhXpyii
j/czo9njofHhqhTr7UEyPun8NVS2QWctLQ86N5zWR3Q0GRoVqqMrJs0cowHTrVw2
9Qr7QBjjBOVbyYmtYxm/DtiKprYV/e6bCAVok015X1sZDd3oCOQNoGlv5XbHJe2o
JFD8GRRy2rkWO/lNwVFDcwec6zC3QwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQCE
goqzjpCpmMgCpszFHwvRaSMbspKtK7wNImUjrSBOfBJsfFulyg1Zgn2nDCK7kQhx
jMJmNIvXbps3yMqQ2cHUkKcKf5t+WldfeT4Vk1Rz6HSA8sd0kgVcIesIaoy2aaXU
VEB/oQziRGyKdN1d4TGYVZXG44CkrzSDvlbmfiTq5tL+kAieznVF3bzHgPZW6hKP
EXC3G/IXrXicFEe6YyE1Rakl62VncYSXiGe/i2XvsiNH3Qlmnx5XS7W0SCN0oAxW
EH9twibauv82DVg1WOkQu8EwFw8hFde9X0Rkiu0qVcuU8lJgFEvPWMDFU5sGB6ZM
gkEKTzMvlZpPbBhg99Jl
-----END CERTIFICATE-----
```

Asia-Pacífico (Hong Kong): ap-east-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq4CCQCO7MJe5Y3VLjAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xOTAyMDMwMjIxMjFaFw00
NTAyMDMwMjIxMjFaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbgwggEsBgcqhkjOOAQBMIIBHwKBgQDvQ9RzVvf4MAwGbqfX
blCvCoVb9957OkLGn/04CowHXJ+vTBR7eyIa6AoXltsQXBOmrJswToFKKxT4gbuw
jK7s9QQX4CmTRWcEgO2RXtZSVjOhsUQMh+yf7Ht4OVL97LWnNfGsX2cwjcRWHYgI
7lvnuBNBzLQHdSEwMNq0Bk76PwIVAMan6XIEEPnwr4e6u/RNnWBGKd9FAoGBAOCG
eSNmxpW4QFu4pIlAykm6EnTZKKHT87gdXkAkfoC5fAfOxxhnE2HezZHp9Ap2tMV5
```

```
8bWNvoPHvoKCQqwfm+OUBlAxC/3vqoVkKL2mG1KgUH9+hrtpMTkwO3RREnKe7I5O
x9qDimJpOihrL4I0dYvy9xUOoz+DzFAW8+ylWVYpA4GFAAKBgQDbnBAKSxWr9QHY
6Dt+EFdGz6lAZLedeBKpaP53Z1DTO34J0C55YbJTwBTFGqPtOLxnUVDlGiD6GbmC
80f3jvogPR1mSmGsydbNbZnbUEVWrRhe+y5zJ3g9qs/DWmDW0deEFvkhWVnLJkFJ
9pdOu/ibRPH1lE2nz6pK7GbOQtLyHTAJBgcqhkjOOAQDAzAAMC0CFQCoJlwGtJQC
cLoM4p/jtVFOj26xbgIUUS4pDKyHaG/eaygLTtFpFJqzWHc=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICSzCCAbQCCQDtQvkVxRvK9TANBgkqhkiG9w0BAQsFADBqMQswCQYDVQQGEwJV
UzETMBEGA1UECBMKV2FzaGluZ3RvbjEQMA4GA1UEBxMHU2VhdHRsZTEYMBYGA1UE
ChMPQW1hem9uLmNvbSBJbmMuMRowGAYDVQQDExFlYzIuYW1hem9uYXdzLmNvbTAe
Fw0xOTAyMDMwMzAwMDZaFw0yOTAyMDIwMzAwMDZaMGoxCzAJBgNVBAYTAlVTMRMw
EQYDVQQIEwpXYXNoaW5ndG9uMRAwDgYDVQQHEwdTZWF0dGxlMRgwFgYDVQQKEw9B
bWF6b24uY29tIEluYy4xGjAYBgNVBAMTEWVjMi5hbWF6b25hd3MuY29tMIGfMA0G
CSqGSIb3DQEBAQUAA4GNADCBiQKBgQC1kkHXYTfc7gY5Q55JJhjTieHAgacaQkiR
Pity9QPDE3b+NXDh4UdP1xdIw73JcIIG3sG9RhWiXVCHh6KkuCTqJfPUknIKk8vs
M3RXflUpBe8Pf+P92pxqPMCz1Fr2NehS3JhhpkCZVGxxwLC5gaG0Lr4rFORubjYY
Rh84dK98VwIDAQABMA0GCSqGSIb3DQEBCwUAA4GBAA6xV9f0HMqXjPHuGILDyaNN
dKcvplNFwDTydVg32MNubAGnecoEBtUPtxBsLoVYXCOb+b5/ZMDubPF9tU/vSXuo
TpYM5Bq57gJzDRaBOntQbX9bgHiUxw6XZWaTS/6xjRJDT5p3S1E0mPI3lP/eJv4o
Ezk5zb3eIf10/sqt4756
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAMoxixvs3YssMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xODA3MjAw
ODQ0NDRaGA8yMTk3MTIyMzA4NDQ0NFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA4T1PNsOg0FDrGlWePoHeOSmOJTA3HCRy5LSbYD33GFU2eBrOIxoU/+SM
rInKu3GghAMfH7WxPW3etIAZiyTDDU5RLcUq2Qwdr/ZpXAWpYocNc/CEmBFtfbxF
z4uwBIN3/drM0RSbe/wP9EcgmNUGQMMZWeAji8sMtwpOblNWAP9BniUG0Flcz6Dp
uPovwDTLdAYT3TyhzlohKL3f6O48TR5yTaV+3Ran2SGRhyJjfh3FRpP4VC+z5LnT
WPQHN74Kdq35UgrUxNhJraMGCzznolUuoR/tFMwR93401GsM9fVA7SW3jjCGF81z
PSzjy+ArKyQqIpLW1YGWDFk3sf08FQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQDK
2/+C3nPMgtyOFX/I3Cyk+Pui44IgOwCsIdNGwuJysdqp5VIfnjegEu2zIMWJSKGO
lMZoQXjffkVZZ97J7RNDW06oB7kj3WVE8a7U4WEOfnO/CbMUf/x99CckNDwpjgW+
```

```
K8V8SzAsQDvYZs2KaE+18GFfLVF1TGUYK2rPSZMHyX+v/TIlc/qUceBycrIQ/kke
jDFsihUMLqgmOV2hXKUpIsmiWMGrFQV4AeV0iXP8L/ZhcepLf1t5SbsGdUA3AUY1
3If8s81uTheiQjwY5t9nM0SY/1Th/tL3+RaEI79VNEVfG1FQ8mgqCK0ar4m0oZJl
tmmEJM7xeURdpBBx36Di
-----END CERTIFICATE-----
```

Asia-Pacífico (Hyderabad): ap-south-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC8DCCArCgAwIBAgIGAXjrQ4+XMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24g
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/
hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYUAAoGBAJCKGBBoxIUxqBk94JHhwZZbgvbP0DAOoHENQWxp/98lI7/
YOfYJOVMJS22aCnHDurofmo5rvNIkgXi7Rztbhu
+lko9rK6DgpmpUwBU0WZtf34aZ2IWNBwHaVhHvWAQf9/46u18dMa2YucK1Wi+Vc+M
+KldrvgXmhym6ErNlzhJyMAkGByqGSM44BAMDLwAwLAIUaaPKxaOHoYvwz709xXpsQueIq+UCFFa/
GpzoDOSokl1057NU/2hnsiW4
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjwLj9CMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
+sFcobrjvcAYm0PNRD8f4R1jAzvoLt2+qGeOTAyO1Httj6cmsYN3AP1hN5iYuppFiYsl2eNPa/
CD0Vg0BAfDFlV5rzjpA0j7TJabVh4kj7JvtD+xYMi6wEQA4x6SPONY4OeZ2+8o/
HS8nucpWDVdPRO6ciWUlMhjmDmwIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAAy6sgTdRkTqELHBeWj69q60xHyUmsWqHAQ
TGGbYP0yP2qfMl0cCImzRI5W0gn8gogdervfeT7nH5ih0TWEy/QDWfkQ601L4erm4yh4YQq8vcqAPSkf04N
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAIVWfPw/X82fMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MDQx
NDMwMjhaGA8yMjAxMTIwODE0MzAyOFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
```

```
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAg29QEFriG+qFEjYW/v62nN70lMJY/Hevx5TtmU/VIYBPQa3HUGTBAbbI
2Tmy8UMpa8kZeaYeI3RAfiQWt0Ws7wUrBuO2Pdp518WDPaJUH7RWEuu1BDDkyZRW
NAMNPCn3ph7Od243IFcLGku7HVekel5poqRpSfojrMasjlf+CvixUeAJbmFoxUHK
kh5unzG2sZyO4wHXcJPQkRf5a8zSTPe9YZP1kXPPEv4p/jTSggaYPxXyS6QVaTlV
zLeLFZ0fesLPMeil3KYQtV7IKLQiEA2F6dxWnxNWQlyMHtdq6PucfEmVx17i/Xza
yNBRo0azY8WUNVkEXrRhp/pU8Nh3GQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU9AO1aZk9RLXk2ZvRVoUxYvQy9uwwgY4GA1UdIwSBhjCBg4AU9AO1
aZk9RLXk2ZvRVoUxYvQy9uyhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAIVWfPw/X82fMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBADexluMRQRftqViahCnauEWGdMvLCBr8A+Yr
6hJq0guoxEk/lahxR137DnfMPuSbi1Rx5QKo7oBrWfG/zsgQUnF2IwHTzwD+i/2m
XCane6FiS5RpK3lGdILq8ZmlhQk+6iI8yoZLr0LCfTh+CLgIKHOknfR5lFzgzAiF
SI8/Q9mm+uvYtSTZECI6Zh57QZPoETAG/yl+9jiOy2lAelqa/k1i+Qo8gMfOc+Pm
dwY7o6fV+oucgRlsdey6VM45LeyILQqv0RXtVzjuowanzmCCFMjgqiO9oZAWu4Oh
+F3unijELo01vZJs8s2N3KGlo3/jtUFTX6RTKShZlAPLwBi5GMI=
-----END CERTIFICATE-----
```

Asia-Pacífico (Yakarta): ap-southeast-3

DSA

```
-----BEGIN CERTIFICATE-----
MIIC8DCCArCgAwIBAgIGAXbVDEikMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24g
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/
hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYUAAoGBAPjuiEx05N3JQ6cVwntJie67D8OuNo4jGRn
+crEtL7YO0jSVB9zGE1ga
+UgRPIaYETL293S8rTJTVgXAqdpBwfaHC6NUzre8U8iJ8FMNnlP9Gw1oUIlgQBjORyynVJexoB31TDZM
+/52g9O/bpq1QqNyKbeIgyBBlc1dAtr1QLnsMAkGByqGSM44BAMDLwAwLAIUK8E6RDIRtwK+9qnaTOBhvO/
njuQCFFocyT1OxK+UDR888oNsdgtif2Sf
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
```

```
MIICMzCCAZygAwIBAgIGAXbVDG2yMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
Vbt0gQ1ebWcur2hSO7PnJifE4OPxQ7RgSAlc4/spJp1sDP+ZrS0LO1ZJfKhXf1R9S3AUwLnsc7b
+IuVXdY5LK9RKqu64nyXP5dx170zoL8loEyCSuRR2fs+04i2QsWBVP+KFNAn7P5L1EHRjkgTO8kjNKviwRV
+OkP9ab5wIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAI4WUy6+DKh0JDSzQEZNyBgNlSoSuC2owtMxCwGB6nBfzzfcekWvs
+87w/g9lNwUnUt0ZHYyh2tuBG6hVJuUEwDJ/z3wDd6wQviLOTF3MITawt9P8siR1hXqLJNxpjRQFZrgHqi
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAMtdyRcH51j9MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA0MDgx
MjM5MTZaGA8yMjAxMDkxMjEyMzkxNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAvUsKCxoH6KXRYJLeYTWAQfaBQeCwhJaR56mfUeFHJE4g8aFjWkiN4uc1
TvOyYNnIZKTHWmzmulmdinWNbwP0GiROHb/i7ro0Hhvnptyyc Gt8ag8affiIbx5X
7ohdwSN2KJ6G0IKflIx7f2NEI0oAMM/9k+T1eVF+MVWzpZoiDp8frLNkqp8+RAgz
ScZsbRfwv3u/if5xJAvdg2nCkIWDMSHEVPoz0lJo7v0ZuDtWWsL1LHnL5ozvsKEk
+ZJyEi23r+U1hIT1NTBdp4yoigNQexedtwCSr7q36oOdDwvZpqYlkLi3uxZ4ta+a
01pzOSTwMLgQZSbKWQrpMvsIAPrxoQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU1GgnGdNpbnL3lLF30Jomg7Ji9hYwgY4GA1UdIwSBhjCBg4AU1Ggn
GdNpbnL3lLF30Jomg7Ji9hahYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAMtdyRcH51j9MBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBACVl00qQlatBKVeiWMrhpczsJroxDxlZTOba
6wTMZk7c3akb6XMOSZFbGaifkebPZqTHEhDlrClM2j9AIlYcCx6YCrTf4cuhn2mD
gcJN33143eOWSaeRY3ee4j+V9ne98y3kO2wLz95VrRgclPFR8po2iWGzGhwUi+FG
q8dXeCH3N0DZgQsSgQWwmdNQXZZej6RHLU/8In5trHKLY0ppnLBjn/UZQbeTyW5q
RJB3GaveXjfgFUWj2qOcDuRGaikdS+dYaLsi5z9cA3FolHzWxx9MOs8io8vKqQzV
XUrLTNWwuhZy88cOlqGPxnoRbw7TmifwPw/cunNrsjUUOgs6ZTk=
-----END CERTIFICATE-----
```

Asia Pacífico (Melbourne): ap-southeast-4

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq
+gAwIBAgIGAXjWF7P2MAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
```

```
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/
hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAPRXSsQP9E3dw8QXKlrgBgEVCprLHdK/bbrMas0XMu1EhOD
+q
+0PcTr8+iwbtoXlY5MCeatWIp1GrXQjVqsF8vQqxlEuRuYKbR3nq4mWwaeGlx9AG5EjQHRa3GQ44wWHOdof0M3NRI1MP
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjSh40SMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
+qWTGAbGsPeMX4hBMjAJUKys2NIRcRZaLM/BCew2FIPVjNtlaj6Gwn9ipU4Mlz3zIwAMWi1AvGMSreppt
+wV6MRtfOjh0Dvj/veJe88aEZJMozNgkJFRS
+WFWsckQeL56tf6kY6QTlNo8V/0CsQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAF7vpPghH0FRo5gu49EArRNPrIvW1egM
wcgkqIwwuXYj+1rhlL+/
iMpQWjdVGEqIZSeXn5fLmdx50eegFCwND837r9e8XYTiQS143Sxt9+Yi6BZ7U7YD8kK9NBWoJxFqUeHdpRCs0O7COjT3
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAN4GTQ64zVs8MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MTMx
MzMzMDBaGA8yMjAxMTIxNzEzMzMwMFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA2BYgeCr+Rk/jIAEDOHS7wJql62vc83QEwjuzk0qOFEReIZzlN1fBRNXK
g0T178Kd3gLYcE59wEFbTe/X5yOA1Lo95x1anSAo7R+Cisf9C2HQuJp+gVb+zx71
lniPF7gHziGpm0M8DdAU/IW+wkZwGbP4z7Hq9+bJ0P2ltvPJ5yxSgkFuDsI9VBHa
CLoprHsCHh2VdP8KcMgQQMmHe1NmBpyTk0ul/aLmQkCQEX6ZIRGOeq228fwlh/t+
Ho+jv87duihVKic6MrL32SlD+maX0LSDUydWdaOLLTGkh7oV7+bFuH6msrXUu+Ur
ZEP1r/MidCWMhfgrFzeTBzOHA97qxQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUcHMd1cHqzmsQ5hpUK3EMLhHdsi4wgY4GA1UdIwSBhjCBg4AUcHMd
1cHqzmsQ5hpUK3EMLhHdsi6hYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAN4GTQ64zVs8MBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAI4PFyVN+7EGSObioiPnv0LL0f70SSzUZJ8p
XO90d4rWea7jIbgZ2AKb+ErynkU9xVg7XQQ5k6KDWgp/4jYFL2dqnt/YAY4PS0un
RSrYElawxLT0BcLn4rcSDC79vQe1xGC5//wDdV6b399COAHRAK6axWYy5w32u9PL
```

```
uw0cIp3Ch8JoNwcgTHKRRGzePmBeR4PNqhHTArG4/dJk6/aUO4OpX0WzI6L67CGY
6Nex3dau+gkLCK93dTEkrXtyXHu4wB0J9zd1w+iQ0SEa9eKc78/NjEsF/FZdGrWC
t57lIMOOXJhQ1kRgSwNeZdQWV1dRakvO6sfcvVYkfj1wAvZvvAw=
-----END CERTIFICATE-----
```

Asia-Pacífico (Bombay): ap-south-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUDLA+x6tTAP3LRTr0z6nOxfsozdMwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE0MTMwMVoXDTI5MDQyODE0MTMwMVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
```

```
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUDLA+x6tT
AP3LRTr0z6nOxfsozdMwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAZ7rYKoAwwiiH1M5GJbrT/BEk3OO2VrEPw8ZxgpqQ/EKlzMlOs/0Cyrmp7
UYyUgYFQe5nq37Z94rOUSeMgv/WRxaMwrLlLqD78cuF9DSkXaZIX/kECtVaUnjk8
BZx0QhoIHOpQocJUSlm/dLeMuE0+0A3HNR6JVktGsUdv9ulmKw==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAPRYyD8TtmC0MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNjAzMDcx
MDQ1MDFaGA8yMTk1MDgxMTEwNDUwMVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA0LSS5I/eCT2PM0+qusorBx67QL26BIWQHd/yF6ARtHBb/1DdFLRqE5Dj
07Xw7eENC+T79mOxOAbeWg91KaODOzw6i9I/2/HpK0+NDEdD6sPKDA1d45jRra+v
CqAjI+nV9Vw91wv7HjMk3RcjWGziM8/hw+3YNIutt7aQzZRwIWlBpcqx3/AFd8Eu
2UsRMSHgkGUW6UzUF+h/U8218XfrauKNGmNKDYUhtmyBrHT+k6J0hQ4pN7fe6h+Z
w9RVHm24BGhlLxLHLmsOIxvbrF277uX9Dxu1HfKfu5D2kimTY7xSZDNLR2dt+kNY
/+iWdIeEFpPT0PLSILt52wP6stF+3QIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBI
E6w+WWC2gCfoJO6c9HMyGLMFEpqZmz1n5IcQt1h9iyO7Vkm1wkJiZsMhXpk73zXf
TPxuXEacTX3SOEa07OIMCFwkusO5f6leOyFTynHCzBgZ3U0UkRVZA3WcpbNB6Dwy
h7ysVlqyT9WZd7EOYm5j5oue2G2xdei+6etgn5UjyWm6liZGrcOF6WPTdmzqa6WG
ApEqanpkQd/HM+hUYex/ZS6zEhd4CCDLgYkIjlrFbFb3pJ1OVLztIfSN5J4Oolpu
JVCfIq5u1NkpzL7ys/Ub8eYipbzI6P+yxXiUSuF0v9b98ymczMYjrSQXIf1e8In3
OP2CclCHoZ8XDQcvvKAh
-----END CERTIFICATE-----
```

Asia-Pacífico (Osaka): ap-northeast-3

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
```

```
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUHTRhxHhBZFOGvTFKxHoy9+f5Hl8wDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2NTQwN1oXDTI5MDQyODE2NTQwN1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUHTRhxHhB
ZFOGvTFKxHoy9+f5Hl8wEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAUZx7DcYbhWNTD4BNGhr5beruT2OUoGHH9J73UKxwdqeb9bH1LIWhIZO0X
/1mjn3bWBgCwfoS8gjZwsVB6fZbNBRy8urdBZJ87xF/4JPBjt7S9oGx/zthDUYrC
yK0Y0v4G0PgiS81CvYLg09LpmYhLSJbXENlkC04v5yxdKxZxyg==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAMn1yPk22ditMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNzA3MTkx
MTEyNThaGA8yMTk2MTIyMjExMTI1OFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
```

```
CgKCAQEArznEYef8IjhrJoazI0QGZkmlmHm/4rEbyQbMNifxjsDE8YWtHNwaM91z
zmyK6Sk/tKlWxcnl3g31iq305ziyFPEewe5Qbwf1iz2cMsvfNBcTh/E6u+mBPH3J
gvGanqUJt6c4IbipdEouIjjnynyVWd4D6erLl/ENijeR1OxVpaqSW5SBK7jms49E
pw3wtbchEl3qsE42Ip4IYmWxqjgaxB7vps91n4kfyzAjUmklcqTfMfPCkzmJCRgp
Vh1C79vRQhmriVKD6BXwfZ8tG3a7mijeDn7kTsQzgO07Z2SAE63PIO48JK8HcObH
tXORUQ/XF1jzi/SIaUJZT7kq3kWl8wIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBj
ThtO9dLvU2QmKuXAhxXjsIdlQgGG3ZGh/Vke4If1ymgLx95v2Vj9Moxk+gJuUSRL
BzFte3TT6b3jPolbECgmAorjj8NxjC17N8QAAI1d0S0gI8kqkG7V8iRyPIFekv+M
pcai1+cIv5IV5qAz8QOMGYfGdYkcoBjsgiyvMJu/2N2UbZJNGWvcEGkdjGJUYYOO
NaspCAFm+6HA/K7BD9zXB1IKsprLgqhiIUgEaW3UFEbThJT+z8UfHG9fQjzzfN/J
nT6vuY/0RRu1xAZPyh2gr5okN/s6rnmh2zmBHU1n8cbCc64MVfXe2g3EZ9Glq/9n
izPrI09hMypJDP04ugQc
-----END CERTIFICATE-----
```

Asia-Pacífico (Seúl): ap-northeast-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUbBSn2UIO6vYk4iNWV0RPxJJtHlgwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
```

```
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTEzMzg0NloXDTI5MDQyODEzMzg0NlowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUbBSn2UIO
6vYk4iNWV0RPxJJtHlgwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAmjTjalG8MGLqWTC2uYqEM8nzI3px1eo0ArvFRsyqQ3fgmWcQpxExqUqRy
l3+2134Kv8dFab04Gut5wlfRtc2OwPKKicmv/IXGN+9bKFnQFjTqif08NIzrDZch
aFT/uvxrIiM+oN2YsHq66GUhO2+xVRXDXVxM/VObFgPERbJpyA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANuCgCcHtOJhMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA5MTQx
NTU3NDRaGA8yMTk1MDIxNzE1NTc0NFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA66iNv6pJPmGM20W8HbVYJSlKcAg2vUGx8xeAbzZIQdpGfkabVcUHGB6m
Gy59VXDMDlrJckDDk6dxUOhmcX9z785TtVZURq1fua9QosdbTzX4kAgHGdp4xQEs
mO6QZqg5qKjBP6xr3+PshfQ1rB8Bmwg0gXEm22CC7o77+7N7Mu2sWzWbiUR7vil4
9FjWS8XmMNwFTlShp4l1TDTevDWW/uYmC30RThM9S4QPvTZ0rAS18hHVam8BCTxa
LHaVCH/Yy52rsz0hM/FlghnSnK105ZKj+b+KIp3adBL8OMCjgc/Pxi0+j3HQLdYE
32+FaXWU84D2iP2gDT28evnstzuYTQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQC1
mA4q+12pxy7By6g3nBk1s34PmWikNRJBwOqhF8ucGRv8aiNhRRye9lokcXomwo8r
KHbbqvtK85l0xUZp/Cx4sm4aTgcMvfJP29jGLclDzeqADIvkWEJ4+xncxSYVlS9x
+78TvF/+8h9U2LnSl64PXaKdxHy2IsHIVRN4GtoaP2Xhpa1S0M328Jykq/571nfN
1WRD1c/fQf1edgzRjhQ4whcAhv7WRRF+qTbfQJ/vDxy8lkiOsvU9XzUaZ0fZSfXX
wXxZamQbONvFcxVHY/0PSiM8nQoUmkkBQuKleDwRWvkoJKYKyr3jvXK7HIWtMrO4
jmXe0aMy3thyK6g5sJVg
-----END CERTIFICATE-----
```

Asia-Pacífico (Singapur): ap-southeast-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUSqP6ih+++5KF07NXngrWf26mhSUwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE0MzAxNFoXDTI5MDQyODE0MzAxNFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUSqP6ih++
+5KF07NXngrWf26mhSUwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAw13BxW11U/JL58j//Fmk7qqtrZTqXmaz1qm2WlIpJpW750MOcP4ux1uPy
eM0RdVZ4jHSMv5gtLAv/PjExBfw9n6vNCk+5GZG4Xec5DoapBZHXmfMo93sjxBFP
4x9rWn0GuwAVO9ukjYPevq2Rerilrq5VvppHtbATVNY2qecXDA==
```

```
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAJVMGw5SHkcvMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEwMjkw
ODU3MTlaGA8yMTk1MDQwMzA4NTcxOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAlaSSLfBl7OgmikjLReHuNhVuvM20dCsVzptUyRbut+KmIEEc24wd/xVy
2RMIrydGedkW4tUjkUyOyfET5OAyT43jTzDPHZTkRSVkYjBdcYbe9o/0Q4P7IVS3
XlvwrUu0qo9nSID0mxMnOoF1l8KAqnn10tQ0W+lNSTkasW7QVzcb+3okPEVhPAOq
MnlY3vkMQGI8zX4iOKbEcSVIzf6wuIffXMGHVC/JjwihJ2USQ8fq6oy686g54P4w
ROg415kLYcodjqThmGJPNUpAZ7MOc5Z4pymFuCHgNAZNvjhZDA842Ojecqm62zcm
Tzh/pNMNeGCRYq2EQX0aQtYOIj7bOQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU6SSB+3qALorPMVNjToM1Bj3oJMswgY4GA1UdIwSBhjCBg4AU6SSB
+3qALorPMVNjToM1Bj3oJMuhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAJVMGw5SHkcvMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAF/0dWqkIEZKg5rca8o0P0VS+tolJJE/FRZO
atHOeaQbWzyac6NEwjYeeV2kY63skJ+QPuYbSuIBLM8p/uTRIvYM4LZYImLGUvoO
IdtJ8mAzq8CZ3ipdMs1hRqF5GRp8lg4w2QpX+PfhnW47iIOBiqSAUkIr3Y3BDaDn
EjeXF6qS4iPIvBaQQ0cvdddNh/pE33/ceghbkZNTYkrwMyBkQlRTTVKXFN7pCRUV
+L9FuQ9y8mP0BYZa5e1sdkwebydU+eqVzsil98ntkhpjvRkaJ5+Drs8TjGaJWlRw
5WuOr8unKj7YxdL1bv7//RtVYVVi296ldoRUYv4SCvJF11z0OdQ=
-----END CERTIFICATE-----
```

Asia Pacífico (Sídney): ap-southeast-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
```

```
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUFxWyAdk4oiXIOC9PxcgjYYh71mwwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE1MjE0M1oXDTI5MDQyODE1MjE0M1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUFxWyAdk4
oiXIOC9PxcgjYYh71mwwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQByjeQe6lr7fiIhoGdjBXYzDfkX0lGGvMIhRh57G1bbceQfaYdZd7Ptc0jl
bpycKGaTvhUdkpMOiV2Hi9dOOYawkdhyJDstmDNKu6P9+b6Kak8He5z3NU1tUR2Y
uTwcz7Ye8Nldx//ws3raErfTI7D6s9m63OX8cAJ/f8bNgikwpw==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAL2bOgb+dq9rMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEwMjkw
OTAwNTdaGA8yMTk1MDQwMzA5MDA1N1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAmRcyLWraysQS8yDC1b5Abs3TUaJabjqWu7d5gHik5Icd6dKl8EYpQSeS
vz6pLhkgO4xBbCRGlgE8LS/OijcZ5HwdrxBiKbicR1YvIPaIyEQQvF5sX6UWkGYw
```

```
Ma5IRGj4YbRmJkBybw+AAV9Icb5LJNOMWPi34OWM+2tMh+8L234v/JA6ogpdPuDr
sM6YFHMZ0NWo58MQ0FnEj2D7H58Ti//vFPl0TaaPWaAIRF85zBiJtKcFJ6vPidqK
f2/SDuAvZmyHC8ZBHg1moX9bR5FsU3QazfbW+c+JzAQWHj2AaQrGSCITxCMlS9sJ
l51DeoZBjnx8cnRe+HCaC4YoRBiqIQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU/wHIo+r5U31VIsPoWoRVsNXGxowwgY4GA1UdIwSBhjCBg4AU/wHI
o+r5U31VIsPoWoRVsNXGxoyhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAL2bOgb+dq9rMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBACobLvj8IxlQyORTz/9q7/VJL509/p4HAeve
92riHp6+Moi0/dSEYPeFTgdWB9W3YCNc34Ss9TJq2D7t/zLGGlbI4wYXU6VJjL0S
hCjWeIyBXUZOZKFCb0DSJeUElsTRSXSFuVrZ9EAwjLvHni3BaC9Ve34iP71ifr75
8Tpk6PEj0+JwiijFH8E4GhcV5chB0/iooU6ioQqJrMwFYnwo1cVZJD5v6D0mu9bS
TMIJLJKv4QQQqPsNdjiB7G9bfkB6trP8fUVYLHLsVlIy5lGx+tgwFEYkG1N8IOO/
2LCawwaWm8FYAFd3IZl04RImNs/IMG7VmH1bf4swHOBHgCN1uYo=
-----END CERTIFICATE-----
```

Asia Pacífico (Tokio): ap-northeast-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
```

```
MIIDITCCAoqgAwIBAgIULgwDh7TiDrPPBJwscqDwiBHkEFQwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTEyMjMxMFoXDTI5MDQyODEyMjMxMFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IULgwDh7Ti
DrPPBJwscqDwiBHkEFQwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBtjAglBde1t4F9EHCZOj4qnY6Gigy07Ou54i+lR77MhbpzE8V28Li9l+YT
QMIn6SzJqU3/fIycIro1OVY1lHmaKYgPGSEZxBenSBHfzwDLRmC9oRp4QMe0BjOC
gepj1lUoiN7OA6PtA+ycNlsP0oJvdBjhvayLiuM3tUfLTrgHbw==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAL9KIB7Fgvg/MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
OTAwMjVaGA8yMTk1MDExNzA5MDAyNVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAz0djWUcmRW85C5CiCKPFiTIvj6y2OuopFxNE5d3Wtab10bm06vnXVKXu
tz3AndG+Dg0zIL0gMlU+QmrSR0PH2PfV9iejfLak9iwdm1WbwRrCEAj5VxPe0Q+I
KeznOtxzqQ5Wo5NLE9bA61sziUAFNVsTFUzphEwRohcekYyd3bBC4v/RuAjCXHVx
40z6AIksnAOGN2VABMlTeMNvPItKOCIeRLlllSqXX1gbtL1gxSW40JWdF3WPB68E
e+/1U3F7OEr7XqmNODOL6yh92QqZ8fHjG+afOL9Y2Hc4g+P1nk4w4iohQOPABqzb
MPjK7B2Rze0f9OEc51GBQu13kxkWWQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU5DS5IFdU/QwYbikgtWvkU3fDwRgwgY4GA1UdIwSBhjCBg4AU5DS5
IFdU/QwYbikgtWvkU3fDwRihYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAL9KIB7Fgvg/MBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAG/N7ua8IE9IMyno0n5T57erBvLTOQ79fIJN
Mf+mKRM7qRRsdg/eumFft0rLOKo54pJ+Kim2cngCWNhkzctRHBV567AJNt4+ZDG5
hDgV0IxWO1+eaLE4qzqWP/9VrO+p3reuumgFZLVpvVpwXBBeBFUf2drUR14aWfI2
L/6VGINXYs7uP8v/2VBS7r6XZRnPBUy/R4hv5efYXnjwA9gq8+a3stC2ur8m5ySl
faKSwE4H320yAyaZWH4gpwUdbUlYgPHtm/ohRtiWPrN7KEG5Wq/REzMIjZCnxOfS
```

```
6KR6PNjlhxBsImQhmBvz6j5PLQxOxBZIpDoiK278e/1Wqm9LrBc=
-----END CERTIFICATE-----
```

Canadá (centro): ca-central-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUIrLgixJJB5C4G8z6pZ5rB0JU2aQwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE1MzU0M1oXDTI5MDQyODE1MzU0M1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUIrLgixJJ
```

```
B5C4G8z6pZ5rB0JU2aQwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBHiQJmzyFAaSYs8SpiRijIDZW2RIo7qBKb/pI3rqK6yOWDlPuMr6yNI81D
IrKGGftg4Z+2KETYU4x76HSf0s//vfH3QA57qFaAwddhKYy4BhteFQl/Wex3xTlX
LiwI07kwJvJy3mS6UfQ4HcvZy219tY+0iyOWrz/jVxwq7TOkCw==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAJNKhJhaJOuMMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNjA3Mjkx
MTM3MTdaGA8yMTk2MDEwMjExMzcxN1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAhDUh6j1ACSt057nSxAcwMaGr8Ez87VA2RW2HyY8l9XoHndnxmP50Cqld
+26AJtltlqHpI1YdtnZ6OrVgVhXcVtbvte0lZ3ldEzC3PMvmISBhHs6A3SWHA9ln
InHbToLX/SWqBHLOX78HkPRaG2k0COHpRy+fG9gvz8HCiQaXCbWNFDHZev9OToNI
xhXBVzIa3AgUnGMalCYZuh5AfVRCEeALG60kxMMC8IoAN7+HG+pMdqAhJxGUcMO0
LBvmTGGeWhi04MUZWfOkwn9JjQZuyLg6B1OD4Y6s0LB2P1MovmSJKGY4JcF8Qu3z
xxUbl7Bh9pvzFR5gJN1pjM2n3gJEPwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQAJ
UNKM+gIIHNk0G0tzv6vZBT+o/vt+tIp8lEoZwaPQh1121iw/I7ZvhMLAigx7eyvf
IxUt9/nf8pxWaeGzi98RbSmbap+uxYRynqe1p5rifTamOsguuPrhVpl12OgRWLcT
rjg/K60UMXRsmg2w/cxV45pUBcyVb5h6Op5uEVAVq+CVns13ExiQL6kk3guG4+Yq
LvP1p4DZfeC33a2Rfre2IHLsJH5D4SdWcYqBsfTpf3FQThH0l0KoacGrXtsedsxs
9aRd7OzuSEJ+mBxmzxSjSwM84Ooh78DjkdpQgv967p3d+8NiSLt3/n7MgnUy6WwB
KtDujDnB+ttEHwRRngX7
-----END CERTIFICATE-----
```

Oeste de Canadá (Calgary) — ca-west-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq
+gAwIBAgIGAYPouptUMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAMITzTJUa6cBsIfdHN69zW/
```

```
aHjUB4r1ZfKb1FMhIp9EZtEf5n+06oXjUG2+dKRSlFQeEK333ehNZsPd6uqey6TYKtHpFb5XRLS8BpqB
+7gnbAd0CBZM5o4NWesSQ1GLnTdQcGZkYG/
QESkbadoCXQTifCujJE682hTDLIVt1d4ewwCQYHKoZIzjgEAwMvADAsAhRJc4gRS/HWTkCR2MESaQEe/
jOMNQIUNoTwLvuPrmGPupPlGiHe0veZiO8=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAYPou9weMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
v4XBVH13ZCMgqlRHMqV8AWI5iO6gFn2A9sN3AZXTMqwtZeiDdebq3k6Wt7ieYvpXTg0qvgsjQIovRZWaBDBJy9x8C2hW
+w9lMQjFHkJ7Jy/
PHCJ69EzebQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAGe9Snkz1A6rHBH6/5kDtYvtPYwhx2sXNxztbhkXErFk40Nw5l4
gvDVtWG7qyb6fAqgoisyAbk8K9LzxSim2S1nmT9vD84B/t/VvwQBylc
+ej8kRxMH7fquZLp7IXfmtBzyUqu6Dpbne+chG2
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALyTn5IHrIZjMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMzEyMDcx
NTM3MDFaGA8yMjAzMDUxMzE1MzcwMVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA1GP5os424BJmGPCKOSgOclP7lzUiB85du03M4hfjzSOszsBpmBGFDLz1
owYHtIxlq3+Vi1Lt5Qlx3id/ov1QyaBPFWXVeklHVXy9vieCcI3TdjGjTl1W/8MM
m3X26QPcsnHM/Kk2wJ7s186MrqmdSsp3SCPpxv4vEG2Q9yR2bXY41hpc2rWlW8qU
D0JGXluvmmAdFnto20l1XWZ6xFen1h60DRugek/ufCbN+ljKy0xLqPoavH0Ybjsb
UpsAsBs7phaoN+X/5hIERfbp5LfVnqq54pNG5KNu4KynfW9+kA/WS4cJ6FTTN5t+
y0P1HvcL+BL2RuDy6T2bB21xw5WqtQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQURTvu/Dd4zDnmS5G5CfVLnmUBNOswgY4GA1UdIwSBhjCBg4AURTvu
/Dd4zDnmS5G5CfVLnmUBNOuhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALyTn5IHrIZjMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAFt523A3Aug6/F8xxyITgA8gkU0btFhlXNSP
U4U2OQ9n0tWI9WqnKNWH3KBxwY5EPitU6b3LM4xc9lDWpz7h2Pto+WhxP9LVKe6f
r8r7teTLCVZ7cfYZHzHg+flZjVpAgzE5BVfrRlj3QKpv0hYT3J1wMtI++Vorq5Nf
aPjzedehJLhmZVALwnfqfLrgv6/gmraP9Vmoa8U4D6AljNiQGYaLwyoPoRm3bUs2
v1Mh9GkEQ1b9+1pFXcqgzJJTGRuiPCyPbECI79FAnx5JM/CkGJV8HlOmjIW1qkK1
Y2qT7wzErrKLJyB53Pw15BdIM1onbDAQreZb0yZQLdoEl/tx7Uk=
-----END CERTIFICATE-----
```

Europa (Fráncfort): eu-central-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUFD5GsmkxRuecttwsCG763m3u63UwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE1NTUyOVoXDTI5MDQyODE1NTUyOVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIEExMQ4IUFD5Gsmkx
RuecttwsCG763m3u63UwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBBh0WaXlBsW56Hqk588MmJxsOrvcKfDjF57RgEDgnGnQaJcStCVWDO9UYO
JX2tdsPw+E7AjDqjsuxYaotLn3Mr3mK0sNOXq9BljBnWD4pARg89KZnZI8FN35HQ
O/LYOVHCknuPL123VmVRNs51qQA9hkPjvw21UzpDLxaUxt9Z/w==
```

```
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAKD+v6LeR/WrMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
OTA4MTlaGA8yMTk1MDExNzA5MDgxOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAka8FLhxs1cSJGK+Q+q/vTf8zVnDAPZ3U6oqppOW/cupCtpwMAQcky8DY
Yb62GF7+C6usniaq/9W6xPn/3o//wti0cNt6MLsiUeHqNl5H/4U/Q/fR+GA8pJ+L
npqZDG2tFi1WMvvGhGgIbScrjR4VO3TuKy+rZXMYvMRk1RXZ9gPhk6evFnviwHsE
jV5AEjxLz3duD+u/SjPp1vloxe2KuWnyC+EKInnka909sl4ZAUh+qIYfZK85DAjm
GJP4W036E9wTJQF2hZJrzsiB1MGyC1WI9veRISd30izZZL6VVXLXUtHwVHnVASrS
zZDVpzj+3yD5hRXsvFigGhY0FCVFnwIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUxC2l6pvJaRflgu3MUdN6zTuP6YcwgY4GA1UdIwSBhjCBg4AUxC2l
6pvJaRflgu3MUdN6zTuP6YehYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAKD+v6LeR/WrMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAIK+DtbUPppJXFqQMv1f2Gky5/82ZwgbbfXa
HBeGSii55b3tsyC3ZW5ZlMJ7Dtnr3vUkiWbV1EUaZGOUlndUFtXUMABCb/coDndw
CAr53XTv7UwGVNe/AFO/6pQDdPxXn3xBhF0mTKPrOGdvYmjZUtQMSVb9lbMWCFfs
w+SwDLnm5NF4yZchIcTs2fdpoyZpOHDXy0xgxO1gWhKTnYbaZOxkJvEvcckxVAwJ
obF8NyJla0/pWdjhlHafEXEN8lyxyTTyOa0BGTuYOBD2cTYYynauVKY4fqHUkr3v
Z6fboaHEd4RFamShM8uvSu6eEFD+qRmvqlcodbpsSOhuGNLzhOQ=
-----END CERTIFICATE-----
```

Europa (Irlanda): eu-west-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
```

```
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUakDaQ1Zqy87Hy9ESXA1pFC116HkwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2MTgxMFoXDTI5MDQyODE2MTgxMFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUakDaQ1Zq
y87Hy9ESXA1pFC116HkwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQADIkn/MqaLGPuK5+prZZ5Ox4bBZLPtreO2C7r0pqU2kPM2lVPyYYydkvP0
lgSmmsErGu/oL9JNztDe2oCA+kNy17ehcsf8cw0uP861czNFKCeU8b7FgBbL+sIm
qi33rAq6owWGi/5uEcfCR+JP7W+oSYVir5r/yDmWzx+BVH5S/g==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAOrmqHuaUt0vMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEwMjkw
OTA2MTlaGA8yMTk1MDQwMzA5MDYxOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAjE7nVu+aHLtzp9FYV25Qs1mvJ1JXD7J0iQ1Gs/RirW9a5ZECCtc4ssnf
zQHq2JRVr0GRchvDrbm1HaP/avtFQR/Thvfltwu9AROVT22dUOTvERdkNzveoFCy
```

```
hf52Rqf0DMrLXG8ZmQPPXPDFAv+sVMWCDftcChxRYZ6mP9O+TpgYNT1krD5PdvJU
7HcXrkNHDYqbsg8A+Mu2hzl0QkvUET83Csg1ibeK54HP9w+FsD6F5W+6ZSHGJ88l
FI+qYKs7xsjJQYgXWfEt6bbckWs1kZIaIOyMzYdPF6ClYzEec/UhIe/uJyUUNfpT
VIsI5OltBbcPF4c7Y20jOIwwI2SgOQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUF2DgPUZivKQR/Zl8mB/MxIkjZDUwgY4GA1UdIwSBhjCBg4AUF2Dg
PUZivKQR/Zl8mB/MxIkjZDWhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAOrmqHuaUt0vMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAGm6+57W5brzJ3+T8/XsIdLTuiBSe5ALgSqI
qnO5usUKAeQsa+kZIJPyEri5i8LEodh46DAF1RlXTMYgXXxl0YggX88XPmPtok17
l4hib/D9/lu4IaFIyLzYNSzsETYWKWoGVe7ZFz60MTRTwY2u8YgJ5dec7gQgPSGj
avB0vTIgoW41G58sfw5b+wjXCsh0nROon79RcQFFhGnvup0MZ+JbljyhZUYFzCli
31jPZiKzqWa87xh2DbAyvj2KZrZtTe2LQ48Z4G8wWytJzxEeZdREe4NoETf+Mu5G
4CqoaPR05KWkdNUdGNwXewydb3+agdCgfTs+uAjeXKNdSpbhMYg=
-----END CERTIFICATE-----
```

Europa (Londres): eu-west-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
```

```
MIIDITCCAoqgAwIBAgIUCgCV/DPxYNND/swDgEKGiC5I+EwwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2MjkxNFoXDTI5MDQyODE2MjkxNFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUCgCV/DPx
YNND/swDgEKGiC5I+EwwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQATPu/sOE2esNa4+XPEGKlEJSgqzyBSQLQc+VWo6FAJhGG9fp7D97jhHeLC
5vwfmtTAfnGBxadfAOT3ASkxnOZhXtnRna460LtnNHm7ArCVgXKJo7uBn6ViXtFh
uEEw4y6p9YaLQna+VC8Xtgw6WKq2JXuKzuhuNKSFaGGw9vRcHg==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANBx0E2bOCEPMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNjA4MTEx
NDU2NDJaGA8yMTk2MDExNTE0NTY0MlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEArYS3mJLGaMrh2DmiPLbqr4Z+xWXTzBWCjOwpsuHE9H6dWUUyl2Bgnu+Z
d8QvW306Yleec45M4F2RA3J4hWHtShzsMlOJVRt+YulGeTf9OCPr26QmIFfs5nD4
fgsJQEry2MBSGA9Fxq3Cw6qkWcrOPsCR+bHOU0XykdKl0MnIbpBf0kTfciAupQEA
dEHnM2J1L2iI0NTLBgKxy5PXLH9weX20BFauNmHH9/J07OpwL20SN5f8TxcM9+pj
Lbk8h1V4KdIwVQpdWkbDL9BCGlYjyadQJxSxz1J343NzrnDM0M4h4HtVaKOS7bQo
Bqt2ruopLRCYgcuFHck/1348iAmbRQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBG
wujwU1Otpi3iBgmhjMClgZyMMn0aQIxMigoFNqXMUNx1Mq/e/Tx+SNaOEAu0n2FF
aiYjvY0/hXOx75ewzZvM7/zJWIdLdsgewpUqOBH4DXFhbSk2TxggSPb0WRqTBxq5
Ed7F7+7GRIeBbRzdLqmISDnfqey8ufW0ks51XcQNomDIRG5s9XZ5KHviDCar8FgL
HngBCdFI04CMagM+pwTO9XN1Ivt+NzUj208ca3oP1IwEAd5KhIhPLcihBQA5/Lpi
h1s3170z1JQ1HZbDrH1pgp+8hSI0DwwDVb3IIH8kPR/J0Qn+hvOl2HOpaUg2Ly0E
pt1RCZe+W7/dF4zsbqwK
-----END CERTIFICATE-----
```

Europa (Milán): eu-south-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAqwCCQCMElHPdwG37jAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xOTA0MjkyMDM1MjJaFw00
NTA0MjkyMDM1MjJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbYwggErBgcqhkjOOAQBMIIBHgKBgQDAkoL4YfdMI/MrQ0oL
NPfeEk94eiCQA5xNOnU7+2eVQtEqjFbDADFENh1p3sh9Q9OoheLFH8qpSfNDWn/0
ktCS909ApTY6Esx1ExjGSeQq/U+SC2JSuuTT4WFMKJ63a/czMtFkEPPnVIjJJJmT
HJSKSsVUgpdDIRvJXuyB0zdB+wIVALQ3OLaVGdlPMNfS1nD/Yyn+32wnAoGAPBQ3
7XHg5NLOS4326eFRUT+4ornQFjJjP6dp3pOBEzpImNmZTtkCNNUKE4Go9hv5T4lh
R0pODvWv0CBupMAZVBP9ObplXPCyEIZtuDqVa7ukPOUpQNgQhLLAqkigTyXVOSmt
ECBj9tu5WNP/x3iTZTHJ+g0rhIqpgh012UwJpKADgYQAAoGAV1OEQPYQUg5/M3xf
6vE7jKTxxyFWEyjKfJK7PZCzOIGrE/swgACy4PYQW+AwcUweSlK/Hx2OaZVUKzWo
wDUbeu65DcRdw2rSwCbBTU342sitFo/iGCV/Gjf+BaiAJtxniZze7J1ob8vOBeLv
uaMQmgOYeZ5e0fl04GtqPl+lhcQwCQYHKoZIzjgEAwMwADAtAhQdoeWLrkm0K49+
AeBK+j6m2h9SKQIVAIBNhS2a8cQVABDCQXVXrc0tOmO8
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICNjCCAZ+gAwIBAgIJAOZ3GEIaDcugMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTEwMjQx
NTE5MDlaGA8yMTk5MDMyOTE1MTkwOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQCjiPgW3vsXRj4JoA16WQDyoPc/eh3QBARaApJEc4nPIGoUolpAXcjFhWplo2O+
ivgfCsc4AU9OpYdAPha3spLey/bhHPRi1JZHRNqScKP0hzsCNmKhfnZTIEQCFvsp
DRp4zr91/WS06/flJFBYJ6JHhp0KwM81XQG59lV6kkoW7QIDAQABMA0GCSqGSIb3
DQEBCwUAA4GBAGLLrY3P+HH6C57dYgtJkuGZGT2+rMkk2n81/abzTJvsqRqGRrWv
XRKRXlKdM/dfiuYGokDGxiC0Mg6TYy6wvsR2qRhtXW1OtZkiHWcQCnOttz+8vpew
wx8JGMvowtuKB1iMsbwyRqZkFYLcvH+Opfb/Aayi20/ChQLdI6M2R5VU
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
```

```
MIIDOzCCAiOgAwIBAgIJAO/+DgYF78KwMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTA0Mjky
MDM1MjJaGA8yMTk4MTAwMjIwMzUyMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAv1ZLV+Z/P6INq+R1qLkzETBg7sFGKPiwHekbpuB6lrRxKHhj8V9vaReM
lnv1Ur5LAPpMPYDsuJ4WoUbPYAqVqyMAo7ikJHCCM1cXgZJefgN6z9bpS+uA3YVh
V/0ipHh/X2hc2S9wvxKWiSHu6Aq9GVpqL035tJQD+NJuqFd+nXrtcw4yGtmvA6wl
5Bjn8WdsP3xOTKjrByYY1BhXpP/f1ohU9jE9dstsRXLa+XTgTPWcWdCS2oRTWPGR
c5Aeh47nnDsyQfP9gLxHeYeQItV/BD9kU/2Hn6mnRg/B9/TYH8qzlRTzLapXp4/5
iNwusrTNexGl8BgvAPrfhjDpdgYuTwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQB7
5ya11K/hKgvaRTvZwVV8GlVZt0CGPtNvOi4AR/UN6TMm51BzUB5nurB4z0R2MoYO
Uts9sLGvSFALJ4otoB77hyNpH3drttU1CVVwal/yK/RQLSon/IoUkaGEbqalu+mH
nYad5IG4tEbmepX456XXcO58MKmnczNbPyw3FRzUZQtI/sf94qBwJ1Xo6XbzPKMy
xjL57LHIZCssD+XPifXay69OFlsCIgLim11HgPkRIHEOXLSf3dsW9r+4CjoZqB/Z
jj/P4TLCxbYCLkvglwaMjgEWF40Img0fhx7yT2X92MiSrs3oncv/IqfdVTiN8OXq
jgnq1bf+EZEZKvb6UCQV
-----END CERTIFICATE-----
```

Europa (París): eu-west-3

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUaC9fX57UDr6u1vBvsCsECKBZQyIwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2MzczOFoXDTI5MDQyODE2MzczOFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUaC9fX57U
Dr6u1vBvsCsECKBZQyIwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQCARv1bQEDaMEzYI0nPlu8GHcMXgmgA94HyrXhMMcaIlQwocGBs6VILGVhM
TXP2r3JFaPEpmXSQNQHvGA13clKwAZbni8wtzv6qXb4L4muF34iQRHF0nYrEDoK7
mMPR8+oXKKuPO/mv/XKo6XAV5DDERdSYHX5kkA2R9wtvyZjPnQ==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJALWSfgHuT/ARMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNzA1MzEx
MTE4MTZaGA8yMTk2MTEwMzExMTgxNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAy5V7KDqnEvF3DrSProFcgu/oL+QYD62b1U+Naq8aPuljJe127Sm9WnWA
EBdOSASkOaQ9fzjCPoG5SGgWKxYoZjsevHpmzjVv9+Ci+F57bSuMbjgUbvbRIFUB
bxQojVoXQPHgK5v433ODxkQ4sjRyUbf4YV1AFdfU7zabC698YgPVOExGhXPlTvco
8mlc631ubw2g52j0lzaozUkHPSbknTomhQIvO6kUfX0e0TDMH4jLDG2ZIrUB1L4r
OWKG4KetduFrRZyDHF6ILZu+s6ywiMicUd+2UllDFC6oas+a8D11hmO/rpWU/ieV
jj4rWAFrsebpn+Nhgy96iiVUGS2LuQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQDE
iYv6FQ6knXCg+svlcaQG9q59xUC5z8HvJZ1+SxzPKKC4PKQdKvIIfE8GxVXqlZG1
cl5WKTFDMapnzb9RV/DTaVzWx3cMYT77vm1Hl1XGjhx611CGcENH1egI3lOTILsa
+KfopuJEQQ9TDMAIkGjhA+KieU/U5Ctv9fdej6d0GC6OEuwKkTNzPWue6UMq8d4H
2xqJboWsE1t4nybEosvZfQJcZ8jyIYcYBnsG13vCLM+ixjuU5MVVQNMY/gBJzqJB
V+U0QiGiuT5cYgY/QihxdHt99zwGaE0ZBC7213NKrlNuLSrqhDI2NLu8NsExqOFy
OmY0v/xVmQUQl26jJXaM
```

```
-----END CERTIFICATE-----
```

Europa (España): eu-south-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC8DCCAq
+gAwIBAgIGAXjwLk46MAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAGG2m8EKmaf5qQqj3Z
+rzSaTaXE3B/R/4A2VuGqRYR7MljPtwdmU6/3CPjCACcZmTIcOAKbFiDHqadQgBZXfzGpzw8Zo
+eYmmk5fXycgnj57PYH1dIWU6I7mCbAah5MZMcmHaTmIsomGrhcnWB8d8qOU7oZ0UWK4lbiAQs1MihoUwCQYHKoZIzjg
WmbaU7YM5GwCFCvIJOesO5hZ8PHC52dAR8WWC6oe
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjwLkiaMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
VvR1+45Aey5zn3vPk6xBm5o9grSDL6D2iAuprQnfVXn8CIbSDbWFhA3fi5ippjKkh3sl8VyCvCOUXKdOaNrYBrPRkrdH
+3m/
rxIUZ2IK1fDlC6sWAjddf6sBrV2w2a78H0H8EwuwiSgttURBjwJ7KPPJCqaqrQIDAQABMA0GCSqGSIb3DQEBBQUAA4GB
+FzqQDzun/
iMMzcFucmLMl5BxEblrFXOz7IIuOeiGkndmrqUeDCykztLku45s7hxdNy4ltTuVAaE5aNBdw5J8U1mRvsKvHLy2ThH6h
+hBgiphYp84DUbWVYeP8YqLEJSqscKscWC
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALWSmO6DvSpQMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MTgx
MzU4NDNaGA8yMjAxMTIyMjEzNTg0M1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
```

```
CgKCAQEAuAAhuSpsHC00/fD2zNlBDpNLRndi9qbHsNeuz3WqN7Samj2aSrM2hS+i
hUxx0BspZj0tZCOsbpPZ+i74NOEQtFeqQoEGvKhB1nJiF4y5I81HDhs5qHvoIivm
7rbbik3zgm1PqS/DmDjVQaXPcD31Rd9ILwBmWEwJqHigyNVlxYtCzTQcrlBrvNZM
dnNgCDAdX/HBEFxx9O12xeu0bSt0s+PJWZ1RTbYrNe7LIH6ntUqHxP/ziQ5trXEZ
uqy7aWk1L8uK4jmyNph0lbaqBa3Y6pYmU1nC27UE4i3fnPB0LSiAr+SrwVvX1g4z
ilo8kr+tbIF+JmcgYLBvO8Jwp+EUqQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUwvGzKJL9A5LReJ4Fxo5K6I20xcowgY4GA1UdIwSBhjCBg4AUwvGz
KJL9A5LReJ4Fxo5K6I20xcqhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALWSmO6DvSpQMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAJAZd31jyoTGLawAD2+v/vQsaB9vZIx5EImi
G8YGkd61uFWeNhAmtrwyE/i6FDSIphDrMHBkvw/D3BsqK+Ev/JOK/VYuaYDx/8fp
H4cwp9jC57CXzdIDREWNf6M9PsHFg2WA9XNNtClOZL5WJiJwel8eDSg+sqJUxE0l
MW+QChq/20F6niyaRK4bXrZq14as7h+F9u3A9xHEOVP7Zk9C2ehrBXzCMLSDt3GV
fEuMea2RxMhozwz34Hkdb6j18qoCfygubulovRNQjKw/cEmgPR16KfZPP5caILVt
9qkYPvePmbiVswZDee73cDymJYxLqILpOZwyXvUH8StiH42FHZQ=
-----END CERTIFICATE-----
```

Europa (Estocolmo): eu-north-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUN1c9U6U/xiVDFgJcYKZB4NkH1QEwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2MDYwM1oXDTI5MDQyODE2MDYwM1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUN1c9U6U/
xiVDFgJcYKZB4NkH1QEwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBTIQdoFSDRHkpqNPUbZ9WXR2O5v/9bpmHojMYZb3Hw46wsaRso7STiGGX/
tRqjIkPUIXsdhZ3+7S/RmhFznmZc8e0bjU4n5vi9CJtQSt+1u4E17+V2bF+D3h/7
wcfE0l3414Q8JaTDtfEf/aF3F0uyBvr4MDMd7mFvAMmDmBPSlA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJALc/uRxg++EnMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xODA0MTAx
NDAwMTFaGA8yMTk3MDkxMzE0MDAxMVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAzwCGJEJIxqtr2PD2a1mA6LhRzKhTBa1AZsg3eYfpETXIVlrpojMfvVoN
qHvGshWLgrGTT6os/3gsaADheSaJKavxwX3X6tJA8fvEGqr3a1C1MffH9hBWbQqC
LbfUTAbkwis4GdTUwOwPjT1Cm3u9R/VzilCNwkj7iQ65AFAI8Enmsw3UGldEsop4
yChKB3KW3WI0FTh0+gD0YtjrqqYJxpGOYBpJp5vwdd3fZ4t1vidmDMs7liv4f9Bx
p0oSmUobU4GUlFhBchK1DukICVQdnOVzdMonYm7s+HtpFbVHR8yf6QoixBKGdSal
mBf7+y0ixjCn0pnC0VLVooGo4mi17QIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQDG
4ONZiixgk2sjJctwbyD5WKLTH6+mxYcDw+3y/F0fWz561YORhP2FNnPOmEkf0Sl/
Jqk4svzJbCbQeMzRoyaya/46d7UioXMHRZam5IaGBhOdQbi97R4VsQjwQj0RmQsq
yDueDyuKTwWLK9KnvI+ZA6e6bRkdNGflK4N8GGKQ+fBhPwVELkbT9f16OJkezeeN
S+F/gDADGJgmPXfjogICb4Kvshq0H5Lm/xZlDULF2g/cYhyNY6EOI/eS5m1I7R8p
D/m6WoyZdpInxJfxW616OMkxQMRVsruLTNGtby3u1g6ScjmpFtvAMhYejBSdzKG4
FEyxIdEjoeO1jhTsck3R
```

```
-----END CERTIFICATE-----
```

Europa (Zúrich): eu-central-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq
+gAwIBAgIGAXjXiKJnMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAYNjaCNg/
cfgQOl1BUj5ClUulqwZ9Q+SfDzPZh9D2C0VbiRANiZoxrV8RdgmzzC5T7VcriVwjwvta2Ch//
b+sZ86E5h0XWWr+BeEjD9cu3eDj12XB5sWEbNHNx49p5Tmtu5r2LDtlL8X/
Rpfalu2Z2OJgjFJWGf7hRwxe456n
+lowCQYHKoZIzjgEAwMvADAsAhRChsLcj4U5CVb2cp5M0RE1XbXmhAIUeGSnH+aiUQIWmPEFja+itWDufIk=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjSGFGiMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
opKZAUusJx2hpgU3pUHhlp9ATh/VeVD582jTd9IY
+8t5MDa6Z3fGliByEiXz0LEHdi8MBacLREu1TwIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAILlpoE3k9o7KdALAxsFJNit
+g3RMzdbiFM+7MA63Nv5fsf+0xgcjSNBElvPCDKFvTJl4QQhToy056llO5GvdS9RK
+H8xrP2mrqngApoKTApv93vHBixgFSn5KrczRO0YSm3OjkqbydU7DFlmkXXR7GYE+5jbHvQHYiT1J5sMu
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALvT012pxTxNMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MTgx
NTEyMDdaGA8yMjAxMTIyMjE1MTIwN1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAyn+Lsnq1ykrfYlZkk6aAAYNReNd9Iw8AUwCBkgOr2eBiBBepYxHwU85N
++moQ+j0EV2VaahBeTLShGZZS1HsyK8+cYT2QzpghIoamcYhrPXyIxlWiRQlaqSg
```

```
OFiE9bsqL3rCF5Vz+tOiTe5W/7ojfOFls6++g7ZpobwJlpMbuJepqyeHMPyjvO5A
age81lJewc4bxo2ntaW0HCqNksqfYB78j6X6kn3PFpX7FaYAwZA+Xx6C7UCY7rNi
UdQzfAo8htfJi4chz7frpUdQ9kl3IOQrsLshBB5fFUjl09NiFipCGBwi+8ZMeSn1
5qwBI01BWXPfG7WX6Owyjhmh6JtE1wIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU8HN4vvJrsZgPQeksMBgJb9xR1yYwgY4GA1UdIwSBhjCBg4AU8HN4
vvJrsZgPQeksMBgJb9xR1yahYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALvT012pxTxNMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAGlHYDtcHpfBvdHx9HeQE8HgNugJUPdEqxun
t9U33p8VFrs+uLPtrOd9HDJEGvvs5h84EUie/oGJxRt7V1Vlid1PvHf6cRmpjgqY
YdggAVkZtY/PnFVmzf2bMVlSQPrqCl7U0zaw2Kvnj4zgX0rZyCetgrRZSUSxotyp
978Wy9ccXwVSeYG/YAr5rJpS6ZH7eRQvUY0IzwFNeaOPgOTEVpcjWlV6+MQEvsEx
W85q+s6AVr49eppEx8SLJsl0C23yB+L+t32tAveQImRWtJMpzZ5cxh/sYgDVeoC0
85H1NK/7H9fAzT1cPu1oHSnB0xYzzHGOAmXmusMfwUk8fL1RQkE=
-----END CERTIFICATE-----
```

Israel (Tel Aviv): il-central-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq+gAwIBAgIGAX0QPi
+9MAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcMB1NlYX
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/
hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAbazCL5XXyPmcw3+oMYQUF5/9YogW6D0FZbYuyPgjOoUwWdl6fjlzWca
pq+l1ezuK2DFOzNTEyPEwwCQYHKoZIzjgEAwMvADAsAhRt1jkpXsvrS
+xTo2M9h2s2uLAhEQIUOZ2FcnTSrshF2EIdixZZwtNv66Q=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAX0QQGVLMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
+S8vOy5hpLoRe4RkOrY0cM3bN07GdEMlin5mU0y1t8y3ct4YewvmkgT42kTyMM
+t1K4S0xsqjXxxS716uGYh7eWtkxrCihj8AbXN/6pa095h
+7TZyl2n83keiNUzM2KoqQVMwIDAQABMA0GCSqGSIb3DQEBBQUAA4GBADwA6VVEIIZD2YL00F12po40xDLzIc9XvqFPS
FmU7H8s62/jD6cOR1A1cClIyZUe1yT1ZbPySCs43J+Thr8i8FSRxzDBSZZi5foW
```

```
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAOVp1h2I9wW7MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MTUx
MjQ0MTJaGA8yMjAxMTIxOTEyNDQxMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA13PkyWvl61iV/SYfO1UFO76UpDfPm2SF/Rz/o33cm699X++EYPxTnoEc
vmWeS0I7eDXc4OCUiToG0sEx0klE0CX1Z1tK6qJ+zgWQLZ9SZEC9H0NsSA6LhrHu
Nq0dzeK3LjhdfcX46/4GqdiptpdTuM4m/hOQ5yx4JMQ/n1sdpv4M5VLRWwWW9Lem
ufb79Id7O9SispxgRsz1KXIjp7N9S4BY7itSXz97uSyzTqEjWZ6mDUhTu3t21GKC
6flALGTTrG2yghEhz53rkvLsvwzjPSSlT6LIf0mrRPzHaf+EdaKoasElE1SHh+ZH
9mI81HywpE+HZ+W+5hBCvjYp90Y1fwIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU58tN2JO+yEGq5JbIXxGi4vRVPyIwgY4GA1UdIwSBhjCBg4AU58tN
2JO+yEGq5JbIXxGi4vRVPyKhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAOVp1h2I9wW7MBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBANBN0e1EqNy4+IU2yQzMJ+Wy5ZIOtTP6GSBR
7muVY1bDeAwtNTEOpwgrZVlC7/xq5Q0LC1y0Z70hHXEf8au7qStaAoUtxzvhTAZI
NC0lwoFU56UFw4N0vZII17iqEfoqRC4PpI3OxqEJHFy0VLlvAzJoKB4QLLqDAYVA
LXCiOLoVT+y9tRYsxw5MyO0Bi6fxQIIADl2bE9xkunTN1Jkkwqo3LxNy/ryz4QWR
8K7jHUItifv4h/hxBKpHEquN8CkdvM9oeGl7I8PFrSFEpGr1euDXY0euZzzYiDBV
m6GpTJgzpVsEuIX52dPcPemwQncoIfZyhWDW85MJUnby2WTEcFo=
-----END CERTIFICATE-----
```

Medio Oriente (Baréin): me-south-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7jCCAq4CCQCVWIgSmP8RhTAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xOTAyMDUxMzA2MjFaFw00
NTAyMDUxMzA2MjFaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbgwggEsBgcqhkjOOAQBMIIBHwKBgQDcwojQfgWdV1QliO0B
8n6cLZ38VE7ZmrjZ9OQV//Gst6S1h7euhC23YppKXi1zovefSDwFU54zi3/oJ++q
PHlP1WGL8IZ34BUgRTtG4TVolvp0smjkMvyRu5hIdKtzjV93Ccx15gVgyk+o1IEG
```

```
fZ2Kbw/Dd8JfoPS7KaSCmJKxXQIVAIZbIaDFRGa2qcMkW2HWASyNDl7bAoGBANtz
IdhfMq+l2I5iofY2oj3HI21Kj3LtZrWEg3W+/4rVhL3lTm0Nne1rl9yGujrjQwy5
Zp9V4A/w9w2O10Lx4K6hj34Eefy/aQnZwNdNhv/FQP7Az0fju+Yl6L13OOHQrL0z
Q+9cF7zEosekEnBQx3v6psNknKgD3Shgx+GO/LpCA4GFAAKBgQCVS7m77nuNAlZ8
wvUqcooxXMPkxJFl54NxAsAul9KP9KN4svm0O3Zrb7t2FOtXRM8zU3TqMpryq1o5
mpMPsZDg6RXo9BF7Hn0DoZ6PJTamkFA6md+NyTJWJKvXC7iJ8fGDBJqTciUHuCKr
12AztQ8bFWsrTgTzPE3p6U5ckcgV1TAJBgcqhkjOOAQDAy8AMCwCFB2NZGWm5EDl
86ayV3c1PEDukgQIAhQow38rQkN/VwHVeSW9DqEshXHjuQ==
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDPDCCAqWgAwIBAgIJAMl6uIV/zqJFMA0GCSqGSIb3DQEBCwUAMHIxCzAJBgNV
BAYTAlVTMRMwEQYDVQQIDApXYXNoaW5ndG9uMRAwDgYDVQQHDAdTZWF0dGxlMSAw
HgYDVQQKDBdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzEaMBgGA1UEAwwRZWMyLmFt
YXpvbmF3cy5jb20wIBcNMTkwNDI2MTQzMjQ3WhgPMjE5ODA5MjkxNDMyNDdaMHIx
CzAJBgNVBAYTAlVTMRMwEQYDVQQIDApXYXNoaW5ndG9uMRAwDgYDVQQHDAdTZWF0
dGxlMSAwHgYDVQQKDBdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzEaMBgGA1UEAwwR
ZWMyLmFtYXpvbmF3cy5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALVN
CDTZEnIeoX1SEYqq6k1BV0ZlpY5y3KnoOreCAE589TwS4MX5+8Fzd6AmACmugeBP
Qk7Hm6b2+g/d4tWycyxLaQlcq81DB1GmXehRkZRgGeRge1ePWd1TUA0I8P/QBT7S
gUePm/kANSFU+P7s7u1NNl+vynyi0wUUrw7/wIZTAgMBAAGjgdcwgdQwHQYDVR0O
BBYEFILtMd+T4YgH1cgc+hVsVOV+480FMIGkBgNVHSMEgZwwgZmAFILtMd+T4YgH
1cgc+hVsVOV+480FoXakdDByMQswCQYDVQQGEwJVUzETMBEGA1UECAwKV2FzaGlu
Z3RvbjEQMA4GA1UEBwwHU2VhdHRsZTEgMB4GA1UECgwXQW1hem9uIFdlYiBTZXJ2
aWNlcyBMTEMxGjAYBgNVBAMMEWVjMi5hbWF6b25hd3MuY29tggkAyXq4hX/OokUw
DAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQsFAAOBgQBhkNTBIFgWFd+ZhC/LhRUY
4OjEiykmbEp6hlzQ79T0Tfbn5A4NYDI2icBP0+hmf6qSnIhwJF6typyd1yPK5Fqt
NTpxxcXmUKquX+pHmIkK1LKDO8rNE84jqxrxRsfDi6by82fjVYf2pgjJW8R1FAw+
mL5WQRFexbfB5aXhcMo0AA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANZkFlQR2rKqMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTAyMDUx
MzA2MjBaGA8yMTk4MDcxMTEzMDYyMFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAy4Vnit2eBpEjKgOKBmyupJzJAiT4fr74tuGJNwwa+Is2vH12jMZn9Il1
```

```
UpvvEUYTIboIgISpf6SJ5LmV5rCv4jT4a1Wm0kjfNbiIlkUi8SxZrPypcw24m6ke
BVuxQZrZDs+xDUYIZifTmdgD50u5YE+TLg+YmXKnVgxBU6WZjbuK2INohi71aPBw
2zWUR7Gr/ggIpf635JLU3KIBLNEmrkXCVSnDFlsK4eeCrB7+UNak+4BwgpuykSGG
Op9+2vsuNqFeU1l9daQeG9roHR+4rIWSPa0opmMxv5nctgypOrE6zKXx2dNXQldd
VULv+WH7s6Vm4+yBeG8ctPYH5GOo+QIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBs
ZcViiZdFdpcXESZP/KmZNDxB/kktlIEIhsQ+MNn29jayE5oLmtGjHj5dtA3XNKlr
f6PVygVTKbtQLQqunRT83e8+7iCZMKI5ev7pITUQVvTUwI+Fc01JkYZxRFlVBuFA
WGZO+98kxCS4n6tTwVt+nSuJr9BJRVC17apfHBgSS8c5OWna0VU/Cc9ka4eAfQR4
7pYSDU3wSRE01cs30q34lXZ629IyFirSJ5TTOIc0osNL7vwMQYj8HOn4OBYqxKy8
ZJyvfXsIPh0Na76PaBIs6ZlqAOflLrjGzxBPiwRM/XrGmF8ze4KzoUqJEnK13O6A
KHKgfiigQZ1+gv5FlyXH
-----END CERTIFICATE-----
```

Medio Oriente (EAU): me-central-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq
+gAwIBAgIGAXjXhqnnMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAW+csuHsWp/7/
pv8CTKFwxsYudxuR6rbWaHCykIeAydXL9AWnphK6yp1ODEMBFl68Xq8Hp23sOWyf8moOhqCom9+0+ovuUFdpvCie86bp
TOZU568Ty1ff3dDWbdRzeNQRHodRG+XEQSizMkAreeWt4kBa+PUwCQYHKoZIzjgEAwMvADAsAhQD3Z
+XGmzKmgaLgGcVX/Qf1+Tn4QIUH1cgksBSVKbWj81tovBMJeKgdYo=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjRrnDjMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
KyA6zyruJQrYy00a6wqLA7eeUzk3bMiTkLsTeDQfrkaZMfBAjGaaOymRo1C3qzE4rIenmahvUplu9ZmLwL1idWXMRX2R
+d2SeoKOKQWoc2UOFZMHYxDue7zkyk1CIRaBukTeY13/
RIrlc6X61zJ5BBtZXlHwayjQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBABTqTy3R6RXKPW45FA+cgo7YZEj/
Cnz5YaoUivRRdX2A83BHuBTvJE2+WX00FTEj4hRVjameE1nENoO8Z7fUVloAFDlDo69fhkJeSvn51D1WRrPnoWGgEfr1
B+Wqm3kVEz/QNcz6npmA6
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAM4h7b1CVhqqMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA0MTEx
MDE1MDNaGA8yMjAxMDkxNTEwMTUwM1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEApybTWfMOhSoMpqPo72eqAmnn1dXGZM+G8EoZXzwHwT/+IHEXNB4q5N6k
tudYLre1bJxuzEw+iProSHjmb9bB9YscRTofjVhBlt35Fc+i8BaMeH94SR/eE8QO
mll8gnLNW3d62lyuhzuyv1e5wVlRqzYw+X2zRH4/wRDOCOpzjKoHIgyPKsMgwsw5
aTZhNMsGxZN9dbkf0iCGeQLDytwU/JTh/HqvSr3VfUOapTJJiyAxoCtZWgp1/7wC
RvOCSMRJobpUqxZgl/VsttwNkikSFz1wGkcYeSQvk+odbnYQckA8tdddoVI56eD4
qtREQvfpMAX5v7fcqLexl5d5vH8uZQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUOadrbTs+OhzwoAgUJ7RqQNdwufkwgY4GA1UdIwSBhjCBg4AUOadr
bTs+OhzwoAgUJ7RqQNdwufmhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAM4h7b1CVhqqMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAICTdAOGEOnII8HaGCpCB8us/hGFaLptJaAf
D5SJAyVy66/mdfjGzE1BKkKxnbxemEVUIzbRidOnyilB+pKwN3edAjTZtWdpVA0V
R/G/qQPmcVljtycBz4VC6SuOUYflGzLH1GZ6GJWbuDtFzw8r7HGdRN1wrEPe3UF2
sMpuVezqnRUdvVRoVQP4jFgNsE7kNvtn2NiPhb/CtrxpcwIQ7r6YeoHcBSheuV1Z
xZDHynC3KUprQGx1+Z9QqPrDf180MaoqAlTl4+W6Pr2NJYrVUFGS/ivYshMg574l
CPU6r4wWZSKwEUXq4BInYX6z6iclp/p/J5QnJp2mAwyi6M+I13Y=
-----END CERTIFICATE-----
```

América del Sur (São Paulo): sa-east-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
```

```
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUX4Bh4MQ86Roh37VDRRX1MNOB3TcwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2NDYwOVoXDTI5MDQyODE2NDYwOVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUX4Bh4MQ8
6Roh37VDRRX1MNOB3TcwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBnhocfH6ZIX6F5K9+Y9V4HFk8vSaaKL5ytw/P5td1h9ej94KF3xkZ5fyjN
URvGQv3kNmNJBoNarcP9I7JIMjsNPmVzqWawyCEGCZImoARxSS3Fc5EAs2PyBfcD
9nCtzMTaKO09Xyq0wqXVYn1xJsE5d5yBDsGrzaTHKjxo61+ezQ==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAMcyoxx4U0xxMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
ODU4MDJaGA8yMTk1MDExNzA4NTgwMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAw45IhGZVbQcy1fHBqzROhO8CsrDzxj/WP4cRbJo/2DAnimVrCCDs5O86
FA39Zo1xsDuJHDlwMKqeXYXkJXHYbcPWc6EYYAnR+PlLG+aNSOGUzsy202S03hT0
B20hWPCqpPp39itIRhG4id6nbNRJOzLm6evHuepMAHR4/OV7hyGOiGaV/v9zqiNA
pMCLhbh2xk0PO35HCVBuWt3HUjsgeks2eEsu9Ws6H3JXTCfiqp0TjyRWapM29OhA
```

```
cRJfJ/d/+wBTz1fkWOZ7TF+EWRIN5ITEadlDTPnF1r8kBRuDcS/lIGFwrOOHLo4C
cKoNgXkhTqDDBDu6oNBb2rS0K+sz3QIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUqBy7D847Ya/w321Dfr+rBJGsGTwwgY4GA1UdIwSBhjCBg4AUqBy7
D847Ya/w321Dfr+rBJGsGTyhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAMcyoxx4U0xxMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBACOoWSBf7b9AlcNrl4lr3QWWSc7k90/tUZal
PlT0G3Obl2x9T/ZiBsQpbUvs0lfotG0XqGVVHcIxF38EbVwbw9KJGXbGSCJSEJkW
vGCtc/jYMHXfhx67Szmftm/MTYNvnzsyQQ3v8y3Rdah+xe1NPdpFrwmfL6xe3pFF
cY33KdHA/3PNLdn9CaEsHmcmj3ctaaXLFIzZhQyyjtsrgGfTLvXeXRokktvsLDS/
YgKedQ+jFjzVJqgr4NjfY/Wt7/8kbbdhzaqlB5pCPjLLzv0zp/XmO6k+JvOePOGh
JzGk5t1QrSju+MqNPFk3+1O7o910Vrhqw1QRB0gr1ExrviLbyfU=
-----END CERTIFICATE-----
```

China (Pekín): cn-north-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIDNjCCAh4CCQD3yZ1w1AVkTzANBgkqhkiG9w0BAQsFADBcMQswCQYDVQQGEwJV
UzEZMBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEg
MB4GA1UEChMXQW1hem9uIFdlYiBTZXJ2aWNlcyBMTEMwIBcNMTUwNTEzMDk1OTE1
WhgPMjE5NDEwMTYwOTU5MTVaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNo
aW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24g
V2ViIFNlcnZpY2VzIExMQzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMWk9vyppSmDU3AxZ2Cy2bvKeK3F1UqNpMuyeriizi+NTsZ8tQqtNloaQcqhto/l
gsw9+QSnEJeYWnmivJWOBdn9CyDpN7cpHVmeGgNJL2fvImWyWe2f2Kq/BL9l7N7C
P2ZT52/sH9orlck1n2zO8xPi7MItgPHQwu3OxsGQsAdWucdxjHGtdchulpo1uJ31
jsTAPKZ3p1/sxPXBBAgBMatPHhRBqhwHO/Twm4J3GmTLWN7oVDds4W3bPKQfnw3r
vtBj/SM4/IgQ3xJslFcl90TZbQbgxIi88R/gWTbs7GsyT2PzstU30yLdJhKfdZKz
/aIzraHvoDTWFaOdy0+OOaECAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAdSzN2+0E
V1BfR3DPWJHWRf1b7zl+1X/ZseW2hYE5r6YxrLv+1VPf/L5I6kB7GEtqhZUqteY7
zAceoLrVu/7OynRyfQetJVGichaaxLNM3lcr6kcxOowb+WQQ84cwrB3keykH4gRX
KHB2rlWSxta+2panSEO1JX2q5jhcFP90rDOtZjlpYv57N/Z9iQ+dvQPJnChdq3BK
5pZlnIDnVVxqRike7BFy8tKyPj7HzoPEF5mh9Kfnn1YoSVu+61lMVv/qRjnyKfS9
c96nE98sYFj0ZVBzXw8Sq4Gh8FiVmFHbQp1peGC19idOUqxPxWsasWxQXO0azYsP
9RyWLHKxH1dMuA==
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
```

```
MIIDCzCCAnSgAwIBAgIJALSOMbOoU2svMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0yMzA3MDQw
ODM1MzlaFw0yODA3MDIwODM1MzlaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
uhhUNlqAZdcWWB/OSDVDGk3OA99EFzOn/mJlmciQ/Xwu2dFJWmSCqEAE6gjufCjQ
q3voxAhC2CF+elKtJW/C0Sz/LYo60PUqd6iXF4h+upB9HkOOGuWHXsHBTsvgkgGA
1CGgel4U0Cdq+23eANr8N8m28UzljjSnTlrYCHtzN4sCAwEAAaOB1DCB0TALBgNV
HQ8EBAMCB4AwHQYDVR0OBBYEFBkZu3wT27NnYgrfH+xJz4HJaNJoMIGOBgNVHSME
gYYwgYOAFBkZu3wT27NnYgrfH+xJz4HJaNJooWCkXjBcMQswCQYDVQQGEwJVUzEZ
MBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEgMB4G
A1UEChMXQW1hem9uIFdlYiBTZXJ2aWNlcyBMTEOCCQC0jjGzqFNrLzASBgNVHRMB
Af8ECDAGAQH/AgEAMA0GCSqGSIb3DQEBCwUAA4GBAECji43p+oPkYqmzll7e8Hgb
oADS0ph+YUz5P/bUCm61wFjlxaTfwKcuTR3ytj7bFLoW5Bm7Sa+TCl3lOGb2taon
2h+9NirRK6JYk87LMNvbS40HGPFumJL2NzEsGUeK+MRiWu+Oh5/lJGii3qw4YByx
SUDlRyNy1jJFstEZjOhs
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAOtrM5XLDSjCMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQx
MDAxNDJaGA8yMTk1MDExNzEwMDE0MlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAvVBz+WQNdPiM9S+aUULOQEriTmNDUrjLWLr7SfaOJScBzis5D5ju0jh1
+qJdkbuGKtFX5OTWTm8pWhInX+hIOoS3exC4BaANoa1A3o6quoG+Rsv72qQf8LLH
sgEi6+LMlCN9TwnRKOToEabmDKorss4zFl7VSsbQJwcBSfOcIwbdRRaW9Ab6uJHu
79L+mBR3Ea+G7vSDrVIA8goAPkae6jY9WGw9KxsOrcvNdQoEkqRVtHo4bs9fMRHU
Etphj2gh4ObXlFN92VtvzD6QBs3CcoFWgyWGvzg+dNG5VCbsiiuRdmii3kcijZ3H
Nv1wCcZoEAqH72etVhsuvNRC/xAP8wIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQA8
ezx5LRjzUU9EYWYhyYIEShFlP1qDHs7F4L46/5lc4pL8FPoQm5CZuAF31DJhYi/b
fcV7i3n++/ymQbCLC6kAg8DUB7NrcROll5ag8d/JXGzcTCnlDXLXx1905fPNa+jI
0q5quTmdmiSi0taeaKZmyUdhrB+a7ohWdSdlokEIOtbH1P+g5yll3bI2leYE6Tm8
LKbyfK/532xJPqO9abx4Ddn89ZEC6vvWVNDgTsxERg992Wi+/xoSw3XxkgAryIv1
zQ4dQ6irFmXwCWJqc6kHg/M5W+z60S/94+wGTXmp+19U6Rkq5jVMLh16XJXrXwHe
4KcgIS/aQGVgjM6wivVA
-----END CERTIFICATE-----
```

China (Ningxia): cn-northwest-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIDNjCCAh4CCQD3yZ1w1AVkTzANBgkqhkiG9w0BAQsFADBcMQswCQYDVQQGEwJV
UzEZMBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEg
MB4GA1UEChMXQW1hem9uIFdlYiBTZXJ2aWNlcyBMTEMwIBcNMTUwNTEzMDk1OTE1
WhgPMjE5NDEwMTYwOTU5MTVaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNo
aW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24g
V2ViIFNlcnZpY2VzIExMQzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMWk9vyppSmDU3AxZ2Cy2bvKeK3F1UqNpMuyeriizi+NTsZ8tQqtNloaQcqhto/l
gsw9+QSnEJeYWnmivJWOBdn9CyDpN7cpHVmeGgNJL2fvImWyWe2f2Kq/BL9l7N7C
P2ZT52/sH9orlck1n2zO8xPi7MItgPHQwu3OxsGQsAdWucdxjHGtdchulpo1uJ31
jsTAPKZ3p1/sxPXBBAgBMatPHhRBqhwHO/Twm4J3GmTLWN7oVDds4W3bPKQfnw3r
vtBj/SM4/IgQ3xJslFcl90TZbQbgxIi88R/gWTbs7GsyT2PzstU30yLdJhKfdZKz
/aIzraHvoDTWFaOdy0+OOaECAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAdSzN2+0E
V1BfR3DPWJHWRf1b7zl+1X/ZseW2hYE5r6YxrLv+1VPf/L5I6kB7GEtqhZUqteY7
zAceoLrVu/7OynRyfQetJVGichaaxLNM3lcr6kcxOowb+WQQ84cwrB3keykH4gRX
KHB2rlWSxta+2panSEO1JX2q5jhcFP90rDOtZjlpYv57N/Z9iQ+dvQPJnChdq3BK
5pZlnIDnVVxqRike7BFy8tKyPj7HzoPEF5mh9Kfnn1YoSVu+61lMVv/qRjnyKfS9
c96nE98sYFj0ZVBzXw8Sq4Gh8FiVmFHbQp1peGC19idOUqxPxWsasWxQXO0azYsP
9RyWLHKxH1dMuA==
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDCzCCAnSgAwIBAgIJALSOMbOoU2svMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0yMzA3MDQw
ODM1MzlaFw0yODA3MDIwODM1MzlaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
uhhUNlqAZdcWWB/OSDVDGk3OA99EFzOn/mJlmciQ/Xwu2dFJWmSCqEAE6gjufCjQ
q3voxAhC2CF+elKtJW/C0Sz/LYo60PUqd6iXF4h+upB9HkOOGuWHXsHBTsvgkgGA
1CGgel4U0Cdq+23eANr8N8m28UzljjSnTlrYCHtzN4sCAwEAAaOB1DCB0TALBgNV
HQ8EBAMCB4AwHQYDVR0OBBYEFBkZu3wT27NnYgrfH+xJz4HJaNJoMIGOBgNVHSME
gYYwgYOAFBkZu3wT27NnYgrfH+xJz4HJaNJooWCkXjBcMQswCQYDVQQGEwJVUzEZ
MBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEgMB4G
A1UEChMXQW1hem9uIFdlYiBTZXJ2aWNlcyBMTEOCCQC0jjGzqFNrLzASBgNVHRMB
Af8ECDAGAQH/AgEAMA0GCSqGSIb3DQEBCwUAA4GBAECji43p+oPkYqmzll7e8Hgb
oADS0ph+YUz5P/bUCm61wFjlxaTfwKcuTR3ytj7bFLoW5Bm7Sa+TCl3lOGb2taon
```

```
2h+9NirRK6JYk87LMNvbS40HGPFumJL2NzEsGUeK+MRiWu+Oh5/lJGii3qw4YByx
SUDlRyNy1jJFstEZjOhs
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAPu4ssY3BlzcMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEyMDMy
MTI5MzJaGA8yMTk1MDUwODIxMjkzMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAsOiGi4A6+YTLzCdIyP8b8SCT2M/6PGKwzKJ5XbSBoL3gsnSWiFYqPg9c
uJPNbiy9wSA9vlyfWMd90qvTfiNrT6vewP813QdJ3EENZOx4ERcf/Wd22tV72kxD
yw1Q3I1OMH4bOItGQAxU5OtXCjBZEEUZooOkU8RoUQOU2Pql4NTiUpzWacNutAn5
HHS7MDc4lUlsJqbN+5QW6fFrcNG/0Mrib3JbwdFUNhrQ5j+Yq5h78HarnUivnX/3
Ap+oPbentv1qd7wvPJu556LZuhfqI0TohiIT1Ah+yUdN5osoaMxTHKKtf/CsSJ1F
w3qXqFJQA0VWsqjFyHXFI32I/GOupwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQCn
Um00QHvUsJSN6KATbghowLynHn3wZSQsuS8E0COpcFJFxP2SV0NYkERbXu0n/Vhi
yq5F8v4/bRA2/xpedLWmvFs7QWlomuXhSnYFkd33Z5gnXPb9vRkLwiMSw4uXls35
qQraczUJ9EXDhrv7VmngIk9H3YsxYrlDGEqh/oz4Ze4ULOgnfkauanHikk+BUEsg
/jsTD+7e+niEzJPihHdsvKFDlud5pakEzyxovHwNJ1GS2I//yxrJFIL91mehjqEk
RLPdNse7N6UvSnuXcOokwu6l6kfzigGkJBxkcq4gre3szZFdCQcUioj7Z4xtuTL8
YMqfiDtN5cbD8R8ojw9Y
-----END CERTIFICATE-----
```

AWS GovCloud (Este de EE. UU): us-gov-east-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
```

```
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIULVyrqjjwZ461qelPCiShB1KCCj4wDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDUwNzE1MjIzNloXDTI5MDUwNjE1MjIzNlowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCpohwYUVPH9I7Vbkb3WMe/JB0Y/bmfVj3VpcK445YBRO9K80al
esjgBc2tAX4KYg4Lht4EBKccLHTzaNi51YEGX1aLNrSmxhz1+WtzNLNUsyY3zD9z
vwX/3k1+JB2dRA+m+Cpwx4mjzZyAeQtHtegVaAytkmqtxQrSCexBxvqRqQIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQU1ZXneBYnPvYXkHVlVjg7918V
gE8wgZkGA1UdIwSBkTCBjoAU1ZXneBYnPvYXkHVlVjg7918VgE+hYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IULVyrqjjw
Z461qelPCiShB1KCCj4wEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBfAL/YZv0y3zmVbXjyxQCsDloeDCJjFKIu3ameEckeIWJbST9LMto0zViZ
puIAf05x6GQiEqfBMk+YMxJfcTmJB4Ebaj4egFlslJPSHyC2xuydHlr3B04INOH5
Z2oCM68u6GGbj0jZjg7GJonkReG9N72kDva/ukwZKgq8zErQVQ==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJALPB6hxFhay8MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xODA0MTAx
MjMyNDlaGA8yMTk3MDkxMzEyMzI0OVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAva9xsI9237KYb/SPWmeCVzi7giKNron8hoRDwlwwMC9+uHPd53UxzKLb
pTgtJWAPkZVxEdl2Gdhwr3SULoKcKmkqE6ltVFrVuPT33La1UufguT9k8ZDDuO9C
hQNHUdSVEuVrK3bLjaSsMOS7Uxmnn7lYT990IReowvnBNBsBlcabfQTBV04xfUG0
/m0XUiUFjOxDBqbNzkEIblW7vK7ydSJtFMSljga54UAVXibQt9EAIF7B8k9l2iLa
```

```
mu9yEjyQy+ZQICTuAvPUEWe6va2CHVY9gYQLA31/zU0VBKZPTNExjaqK4j8bKs1/
7dOV1so39sIGBz21cUBec1o+yCS5SwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBt
hO2W/Lm+Nk0qsXW6mqQFsAou0cASc/vtGNCyBfoFNX6aKXsVCHxq2aq2TUKWENs+
mKmYu1lZVhBOmLshyllh3RRoL3Ohp3jCwXytkWQ7ElcGjDzNGc0FArzB8xFyQNdK
MNvXDi/ErzgrHGSpcvmGHiOhMf3UzChMWbIr6udoDlMbSIO7+8F+jUJkh4Xl1lKb
YeN5fsLZp7T/6YvbFSPpmbn1YoE2vKtuGKxObRrhU3h4JHdp1Zel1pZ6lh5iM0ec
SD11SximGIYCjfZpRqI3q50mbxCd7ckULz+UUPwLrfOds4VrVVSj+x0ZdY19Plv2
9shw5ez6Cn7E3IfzqNHO
-----END CERTIFICATE-----
```

AWS GovCloud (Oeste de EE. UU): us-gov-west-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUe5wGF3jfb7lUHzvDxmM/ktGCLwwwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDUwNzE3MzAzMloXDTI5MDUwNjE3MzAzMlowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
```

```
A4GNADCBiQKBgQCpohwYUVPH9I7Vbkb3WMe/JB0Y/bmfVj3VpcK445YBRO9K80al
esjgBc2tAX4KYg4Lht4EBKccLHTzaNi51YEGX1aLNrSmxhz1+WtzNLNUsyY3zD9z
vwX/3k1+JB2dRA+m+Cpwx4mjzZyAeQtHtegVaAytkmqtxQrSCexBxvqRqQIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQU1ZXneBYnPvYXkHVlVjg7918V
gE8wgZkGA1UdIwSBkTCBjoAU1ZXneBYnPvYXkHVlVjg7918VgE+hYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUe5wGF3jf
b7lUHzvDxmM/ktGCLwwwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQCbTdpx1Iob9SwUReY4exMnlwQlmkTLyA8tYGWzchCJOJJEPfsW0ryy1A0H
YIuvyUty3rJdp9ib8h3GZR71BkZnNddHhy06kPs4p8ewF8+d8OWtOJQcI+ZnFfG4
KyM4rUsBrljpG2aOCm12iACEyrvgJJrS8VZwUDZS6mZEnn/lhA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANCOF0Q6ohnuMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA5MTAx
OTQyNDdaGA8yMTk1MDIxMzE5NDI0N1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAzIcGTzNqie3f1olrrqcfzGfbymSM2QfbTzDIOG6xXXeFrCDAmOq0wUhi
3fRCuoeHlKOWAPu76B9os71+zgF22dIDEVkpqHCjBrGzDQZXXUwOzhm+PmBUI8Z1
qvbVD4ZYhjCujWWzrsX6Z4yEK7PEFjtf4M4W8euw0RmiNwjy+knIFa+VxK6aQv94
lW98URFP2fD84xedHp6ozZlr3+RZSIFZsOiyxYsgiwTbesRMI0Y7LnkKGCIHQ/XJ
OwSISWaCddbu59BZeADnyhl4f+pWaSQpQQ1DpXvZAVBYvCH97J1oAxLfH8xcwgSQ
/se3wtn095VBt5b7qTVjOvy6vKZazwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQA/
S8+a9csfASkdtQUOLsBynAbsBCH9Gykq2m8JS7YE4TGvqlpnWehz78rFTzQwmz4D
fwq8byPkl6DjdF9utqZ0JUo/Fxelxom0h6oievtBlSkmZJNbgc2WYm1zi6ptViup
Y+4S2+vWZyg/X1PXD7wyRWuETmykk73uEyeWFBYKCHWsO9sI+62O4Vf8Jkuj/cie
1NSJX8fkervfLrZSHBYhxLbL+actVEo00tiyZz8GnhgWx5faCY38D/k4Y/j5Vz99
7lUX/+fWHT3+lTL8ZZK7fOQWh6NQpI0wTP9KtWqfOUwMIbgFQPoxkP00TWRmdmPz
WOwTObEf9ouTnjG9OZ20
-----END CERTIFICATE-----
```

Roles de identidad de instancia

Cada instancia que lance tiene un rol de identidad de instancia que representa su identidad. Un rol de identidad de instancia es un tipo de rol de IAM. Los servicios y las características de AWS

integrados para usar el rol de identidad de instancia pueden usarlo para identificar la instancia en el servicio.

Las credenciales de rol de identidad de instancia están disponibles en el servicio de metadatos de instancia (IMDS) en `/identity-credentials/ec2/security-credentials/ec2-instance`. Las credenciales incluyen un par de claves de acceso temporal de AWS y un token de sesión. Se utilizan para firmar las solicitudes de Sigv4 de AWS a los servicios de AWS que utilizan el rol de identidad de instancia. Las credenciales están presentes en los metadatos de la instancia independientemente de si un servicio o una característica que utiliza los roles de identidad de la instancia está habilitado en la instancia.

Los roles de identidad de instancia se crean automáticamente cuando se inicia una instancia, no tienen ningún documento de política de confianza de roles y no están sujetos a ninguna política de identidad o recursos.

Servicios admitidos

Los siguientes servicios de AWS utilizan el rol de identidad de instancia:

- Amazon EC2: la conexión de instancias EC2 utiliza el rol de identidad de instancia para actualizar las claves de host de una instancia de Linux.
- Amazon GuardDuty: el monitoreo de tiempo de ejecución utiliza el rol de identidad de instancia para permitir que el agente de tiempo de ejecución envíe telemetría de seguridad al punto de conexión de VPC de GuardDuty.
- AWS Security Token Service (AWS STS): las credenciales del rol de identidad de instancia se pueden usar con la acción `GetCallerIdentity`de AWS STS.
- AWS Systems Manager: cuando se utiliza la configuración de la administración de host predeterminada, AWS Systems Manager utiliza la identidad proporcionada por el rol de identidad de instancia para registrar las instancias de EC2. Tras identificar la instancia, Systems Manager puede pasar el rol de IAM de `AWSSystemsManagerDefaultEC2InstanceManagementRole` a la instancia.

Los roles de identidad de instancia no se pueden usar con otros servicios o características de AWS porque no están integrados con los roles de identidad de instancia.

ARN de rol de identidad de instancia

El ARN de rol de identidad de instancia tiene el siguiente formato:

```
arn:aws-partition:iam::account-number:assumed-role/aws:ec2-instance/instance-id
```

Por ejemplo:

```
arn:aws:iam::0123456789012:assumed-role/aws:ec2-instance/i-0123456789example
```

Para más información acerca de los ARN, consulte Nombres de recursos de Amazon (ARN) en la guía de referencia de usuario de IAM.

Ejecución de comandos en la instancia de Amazon EC2 durante la inicialización

Al iniciar una instancia de Amazon EC2, los datos de usuario se pueden transmitir a la instancia utilizada para realizar tareas de configuración automáticas o ejecutar scripts después de que se inicie la instancia.

Si le interesan escenarios de automatización más complejos, puede plantearse el uso de AWS CloudFormation y AWS OpsWorks. Para más información, consulte los siguientes temas:

- Implementación de aplicaciones en Amazon EC2 mediante AWS CloudFormation la Guía del usuario de AWS CloudFormation.
- Guía del usuario de AWS OpsWorks.

En las instancias de Linux, puede transferir dos tipos de datos de usuario a Amazon EC2: scripts de intérprete de comandos y directivas cloud-init. También puede pasar estos datos en el asistente de inicialización de instancias como texto sin formato, como archivo (esto resulta útil para iniciar instancias con las herramientas de la línea de comandos) o como texto codificado en base64 (para llamadas a la API).

En las instancias de Windows, los agentes de inicialización gestionan los scripts de datos de usuario. En las siguientes secciones se describen las diferencias en la forma en que se gestionan los datos de los usuarios en cada sistema operativo.

Cómo gestiona Amazon EC2 los datos de usuario de las instancias de Linux

En los ejemplos siguientes, los comandos de Install a LAMP server on Amazon Linux 2 se convierten en un script de intérprete de comandos y un conjunto de directivas de cloud-init que se ejecutan cuando se inicia la instancia. En cada ejemplo, los datos de usuario ejecutan las tareas siguientes:

- Se actualizan los paquetes de software de distribución.
- Se instalan los paquetes del servidor web `php` y `mariadb` necesarios.
- El servicio `httpd` se inicia y se activa mediante el comando systemctl.
- Se añade `ec2-user` al grupo apache.
- Se establecen los permisos de archivo y la propiedad adecuados para el directorio web y los archivos que contiene.
- Se crea una página web sencilla para probar el servidor web y el motor PHP.

Contenido

Requisitos previos

Los ejemplos de este tema suponen lo siguiente:

- Su instancia tiene un nombre de DNS público al que se puede acceder desde Internet.
- El grupo de seguridad asociado a la instancia está configurado para permitir el tráfico SSH (puerto 22) para que pueda conectarse a la instancia y ver los archivos de registro de salida.
- La instancia se inicia con una AMI de Amazon Linux 2. Estas instrucciones son para usar con Amazon Linux 2; es posible que los comandos y directivas no funcionen con otras distribuciones de Linux. Para obtener más información acerca de otras distribuciones de Linux, por ejemplo su compatibilidad con cloud-init, consulte la documentación específica.

Scripts de shell y datos de usuario

Si está familiarizado con el scripting desde el shell, esta es la forma más sencilla y completa de enviar instrucciones a una instancia tras su inicialización. Si estas tareas se agregan en el momento del arranque, aumentará la cantidad de tiempo necesario para arrancar la instancia. Conceda algunos minutos extra para que estas tareas se completen antes de probar que el script de usuario ha finalizado satisfactoriamente.

> **Important**
>
> De forma predeterminada, los scripts de datos de usuario y las directivas de cloud-init solo se ejecutan durante el ciclo de arranque cuando se inicia una instancia por primera vez. Puede actualizar la configuración para asegurarse de que los scripts de datos de usuario y las directivas de cloud-init se ejecuten cada vez que reinicie la instancia. Para obtener más información, consulte ¿Cómo puedo utilizar los datos de usuario para ejecutar automáticamente un script con cada reinicio de mi instancia de Amazon EC2 Linux? en el AWSCentro de Conocimientos.

Los scripts de shell de datos de usuario deben comenzar por los caracteres `#!` y la ruta del intérprete que se desea que lea el script (normalmente /bin/bash). Para obtener una introducción a las secuencias de intérprete de comandos, consulte el Manual de referencia de Bash en el sitio web del Sistema operativo GNU.

Los scripts que se introducen como datos de usuario se ejecutan como el usuario raíz; por consiguiente, no use el comando sudo en el script. Recuerde que los archivos que cree serán propiedad del usuario raíz; si necesita que usuarios no raíz tengan acceso a los archivos, tendrá que modificar los permisos consecuentemente en el script. Asimismo, como el script no se ejecuta de forma interactiva, no puede incluir comandos que requieran respuestas de los usuarios (como yum update sin la marca `-y`).

Si utiliza una API de AWS, incluida la CLI de AWS, en un script de datos del usuario, debe utilizar un perfil de instancia al iniciar la instancia. Un perfil de instancia proporciona las credenciales de AWS adecuadas requeridas por el script de datos del usuario para emitir la llamada a la API. Para obtener más información, consulte Uso de perfiles de instancia en la Guía del usuario de IAM. Los permisos que asigne al rol de IAM dependen de los servicios a los que llame con la API. Para obtener más información, consulte Roles de IAM para Amazon EC2.

El archivo de registro de salida cloud-init captura la salida para que pueda depurar sus scripts fácilmente después de la inicialización si una instancia no se comporta de la manera prevista. Para ver el archivo de registro, conéctese a la instancia y abra `/var/log/cloud-init-output.log`.

Cuando se procesa un script de datos del usuario, se copia y se ejecuta desde `/var/lib/cloud/instances/instance-id/`. El script no se elimina después de ejecutarse. Asegúrese de eliminar los scripts de `/var/lib/cloud/instances/instance-id/` antes de crear una AMI desde la instancia. De lo contrario, el script estará en este directorio en cualquier instancia iniciada desde la AMI.

Datos de usuario y la consola

Puede especificar los datos de usuario de la instancia al iniciar la instancia. Si el volumen raíz de la instancia es un volumen de EBS, también puede detener la instancia y actualizar los datos de usuario.

Especificar los datos de usuario de la instancia durante la inicialización

Siga el procedimiento para iniciar una instancia. El campo User data (Datos de usuario) se encuentra en la sección Detalles avanzados del asistente de inicialización de instancias. Ingrese el script de shell en el campo User data y, a continuación, complete el procedimiento de inicialización de instancias.

En el script de ejemplo siguiente, el script crea y configura nuestro servidor web.

```
#!/bin/bash
 yum update -y
 amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2
 yum install -y httpd mariadb-server
 systemctl start httpd
 systemctl enable httpd
 usermod -a -G apache ec2-user
 chown -R ec2-user:apache /var/www
 chmod 2775 /var/www
 find /var/www -type d -exec chmod 2775 {} \;
 find /var/www -type f -exec chmod 0664 {} \;
 echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php
```

Conceda tiempo suficiente para que la instancia se lance y ejecute los comandos del script y después compruebe si el script ha completado las tareas deseadas.

Para nuestro ejemplo, en un explorador web, escriba la URL del archivo PHP de prueba que ha creado el script. Esta URL es la dirección DNS pública de la instancia seguida de una barra diagonal y el nombre del archivo.

```
http://my.public.dns.amazonaws.com/phpinfo.php
```

Debería ver la página de información PHP. Si no puede ver la página de información de PHP, compruebe que el grupo de seguridad que usa contiene una regla que permite el tráfico HTTP (puerto 80). Para obtener más información, consulte Agregar reglas a un grupo de seguridad.

(Opcional) Si el script no llevó a cabo las tareas que esperaba o si simplemente desea verificar que las completó sin errores, conéctese a la instancia examine el archivo de registro de salida de cloud-init (`/var/log/cloud-init-output.log`) y busque los mensajes de error en el resultado.

Para obtener información adicional sobre depuración, puede crear un archivo multiparte Mime que incluya una sección de datos cloud-init con la directiva siguiente:

```
output : { all : '| tee -a /var/log/cloud-init-output.log' }
```

Esta directiva envía el resultado de los comandos del script a `/var/log/cloud-init-output.log`. Para obtener más información sobre los formatos de datos de cloud-init y cómo crear un archivo multiparte Mime, consulte cloud-init Formats.

Visualizar y actualizar los datos de usuario de la instancia

Para poder actualizar los datos de usuario de la instancia, primero debe detener la instancia. Si la instancia se está ejecutando, podrá ver los datos del usuario, pero no modificarlos.

> **Warning**
>
> Cuando detiene una instancia, se borran los datos contenidos en todos los volúmenes de almacén de instancias. Para conservar los datos de los volúmenes del almacén de instancias, asegúrese de realizar una copia de seguridad de ellos en un almacenamiento persistente.

Para modificar los datos de usuario de la instancia

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

2. En el panel de navegación, seleccione Instancias.
3. Seleccione la instancia y elija Instance State (Estado de la instancia) y Stop instance (Detener instancia). Si esta opción está desactivada, la instancia ya está detenida o bien su dispositivo raíz es un volumen de almacén de instancias.
4. Cuando se le pida que confirme, elija Stop. Puede que transcurran unos minutos hasta que la instancia se detenga.
5. Con la instancia aún seleccionada, elija Actions (Acciones), Instance Settings (Configuración de la instancia) y Edit user data (Editar datos del usuario).
6. Modifique los datos de usuario según sea necesario y después elija Save (Guardar).
7. Inicie la instancia. Los nuevos datos de usuario son visibles en su instancia tras reiniciarla; sin embargo, los scripts de datos de usuario no se ejecutan.

Directivas cloud-init y datos de usuario

El paquete cloud-init configura aspectos específicos de una nueva instancia de Amazon Linux cuando se inicia; lo más notable es que configura el archivo `.ssh/authorized_keys` para el usuario ec2-user, de forma que puede iniciar sesión con su propia clave privada. Para obtener más información sobre las tareas de configuración que el paquete cloud-init lleva a cabo para las instancias de Amazon Linux, consulte Using cloud-init on Amazon Linux 2 en la Guía del usuario de Amazon Linux 2.

Las directivas de usuario cloud-init se pueden pasar a una instancia durante la inicialización del mismo modo que se pasa un script, si bien la sintaxis es diferente. Para obtener más información sobre el inicio en la nube, visite http://cloudinit.readthedocs.org/en/latest/index.html.

> **Important**
>
> De forma predeterminada, los scripts de datos de usuario y las directivas de cloud-init solo se ejecutan durante el ciclo de arranque cuando se inicia una instancia por primera vez. Puede actualizar la configuración para asegurarse de que los scripts de datos de usuario y las directivas de cloud-init se ejecuten cada vez que reinicie la instancia. Para obtener más información, consulte ¿Cómo puedo utilizar los datos de usuario para ejecutar automáticamente un script con cada reinicio de mi instancia de Amazon EC2 Linux? en el AWSCentro de Conocimientos.

Si estas tareas se agregan en el momento del arranque, aumentará la cantidad de tiempo necesario para arrancar una instancia. Conceda unos cuantos minutos extra para que estas tareas se completen antes de probar que las directivas de datos de usuario han finalizado.

Para pasar directivas cloud-init a una instancia con datos de usuario

1. Siga el procedimiento para iniciar una instancia. El campo User data (Datos de usuario) se encuentra en la sección Detalles avanzados del asistente de inicialización de instancias. Ingrese el texto de la directiva de inicio en la nube en el campo User data y, a continuación, complete el procedimiento de inicialización de instancias.

   En el ejemplo siguiente, las directivas crean y configuran un servidor web en Amazon Linux 2. La línea `#cloud-config` de la parte superior es obligatoria para poder identificar los comandos como directivas cloud-init.

   ```
   #cloud-config
    repo_update: true
    repo_upgrade: all

    packages:
    - httpd
    - mariadb-server

    runcmd:
    - [ sh, -c, "amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2" ]
    - systemctl start httpd
    - sudo systemctl enable httpd
    - [ sh, -c, "usermod -a -G apache ec2-user" ]
    - [ sh, -c, "chown -R ec2-user:apache /var/www" ]
    - chmod 2775 /var/www
    - [ find, /var/www, -type, d, -exec, chmod, 2775, {}, \; ]
    - [ find, /var/www, -type, f, -exec, chmod, 0664, {}, \; ]
    - [ sh, -c, 'echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php' ]
   ```

2. Conceda tiempo suficiente para que la instancia se lance y ejecute las directivas en los datos de usuario y después compruebe si las directivas han completado las tareas deseadas.

   Para este ejemplo, en un explorador web, escriba la URL del archivo PHP de prueba que han creado las directivas. Esta URL es la dirección DNS pública de la instancia seguida de una barra diagonal y el nombre del archivo.

```
http://my.public.dns.amazonaws.com/phpinfo.php
```

Debería ver la página de información PHP. Si no puede ver la página de información de PHP, compruebe que el grupo de seguridad que usa contiene una regla que permite el tráfico HTTP (puerto 80). Para obtener más información, consulte Agregar reglas a un grupo de seguridad.

3. (Opcional) Si las directivas no llevaron a cabo las tareas que esperaba o si simplemente desea verificar que las completaron sin errores, conéctese a la instancia, examine el archivo de registro de salida de cloud-init (`/var/log/cloud-init-output.log`) y busque los mensajes de error en el resultado. Para obtener información adicional sobre depuración, puede agregar las líneas siguientes a las directivas:

```
output : { all : '| tee -a /var/log/cloud-init-output.log' }
```

Esta directiva envía el resultado de runcmd a `/var/log/cloud-init-output.log`.

Datos de usuario y las AWS CLI

Puede usar la AWS CLI para especificar, modificar y ver los datos de usuario de la instancia. Para obtener más información acerca de cómo ver los datos de usuario de la instancia usando los metadatos de la instancia, consulte Recuperación de los datos de usuario de la instancia desde su instancia.

En Windows puede utilizar las AWS Tools for Windows PowerShell en vez de la AWS CLI. Para obtener más información, consulte Datos de usuario y las Tools for Windows PowerShell.

Ejemplo: Especificar datos de usuario durante la inicialización

Para especificar los datos de usuario cuando lance una instancia, ejecute el comando run-instances con el parámetro `--user-data`. Con run-instances, la AWS CLI lleva a cabo la codificación en base64 de los datos de usuario automáticamente.

En el siguiente ejemplo se muestra cómo especificar un script como cadena en la línea de comandos:

```
aws ec2 run-instances --image-id ami-abcd1234 --count 1 --instance-type m3.medium \
 --key-name my-key-pair --subnet-id subnet-abcd1234 --security-group-ids sg-abcd1234 \
 --user-data echo user data
```

En el siguiente ejemplo se muestra cómo especificar un script utilizando un archivo de texto. Asegúrese de utilizar el prefijo `file://` para especificar el archivo.

```
aws ec2 run-instances --image-id ami-abcd1234 --count 1 --instance-type m3.medium \
 --key-name my-key-pair --subnet-id subnet-abcd1234 --security-group-ids sg-abcd1234 \
 --user-data file://my_script.txt
```

En el siguiente ejemplo se muestra un archivo de texto con un script de shell.

```
#!/bin/bash
 yum update -y
 service httpd start
 chkconfig httpd on
```

Ejemplo: Modificar los datos de usuario de una instancia detenida

Puede modificar los datos de usuario de una instancia detenida con el comando modify-instance-attribute. Con modify-instance-attribute, la AWS CLI no lleva a cabo la codificación en base64 de los datos de usuario automáticamente.

- En un equipo Linux utilice el comando base64 para codificar los datos de usuario.

  ```
  base64 my_script.txt >my_script_base64.txt
  ```

- En un equipo Windows, use el comando certutil para codificar los datos de usuario. Para poder usar este archivo con la AWS CLI, debe eliminar la primera línea (BEGIN CERTIFICATE) y la última (END CERTIFICATE).

  ```
  certutil -encode my_script.txt my_script_base64.txt
   notepad my_script_base64.txt
  ```

Use los parámetros `--attribute` y `--value` para usar el archivo de texto codificado para especificar los datos de usuario. Asegúrese de utilizar el prefijo `file://` para especificar el archivo.

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --attribute
 userData --value file://my_script_base64.txt
```

Ejemplo: Borrar los datos de usuario de una instancia detenida

Para eliminar los datos de usuario existentes, utilice el comando modify-instance-attribute de la siguiente manera:

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --user-data Value=
```

Ejemplo: Ver los datos de usuario

Para recuperar los datos de usuario de una instancia, utilice el comando describe-instance-attribute. Con describe-instance-attribute, la AWS CLI no lleva a cabo la descodificación en base64 de los datos de usuario automáticamente.

```
aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --attribute
 userData
```

El siguiente ejemplo es una salida de ejemplo donde se muestran los datos del usuario codificados en base64.

```
{
 "UserData": {
     "Value":
 "IyEvYmluL2Jhc2gKeXVtIHVwZGF0ZSAteQpzZXJ2aWNlIGh0dHBkIHN0YXJ0CmNoa2NvbmZpZyBodHRwZCBvbg=="
 },
 "InstanceId": "i-1234567890abcdef0"
 }
```

- En un equipo Linux, use la opción `--query` para obtener los datos de usuario codificados y el comando base64 para descodificarlos.

  ```
  aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --attribute
   userData --output text --query "UserData.Value" | base64 --decode
  ```

- En un equipo Windows, use la opción `--query` para obtener los datos de usuario codificados y el comando certutil para descodificarlos. Observe que el resultado codificado se guarda en un archivo y el resultado descodificado, en otro.

  ```
  aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --attribute
   userData --output text --query "UserData.Value" >my_output.txt
   certutil -decode my_output.txt my_output_decoded.txt
   type my_output_decoded.txt
  ```

A continuación, se muestra un ejemplo del resultado.

```
#!/bin/bash
 yum update -y
 service httpd start
 chkconfig httpd on
```

Combinación de scripts de shell y directivas cloud-init

De forma predeterminada, solo puede incluir un tipo de contenido en los datos de usuario a la vez. Sin embargo, puede utilizar los tipos de contenido `text/cloud-config` y `text/x-shellscript` en un archivo MIME de varias partes para incluir tanto un script de shell como las directivas cloud-init en los datos de usuario.

A continuación se muestra el formato MIME de varias partes.

```
Content-Type: multipart/mixed; boundary="//"
 MIME-Version: 1.0

 --//
 Content-Type: text/cloud-config; charset="us-ascii"
 MIME-Version: 1.0
 Content-Transfer-Encoding: 7bit
 Content-Disposition: attachment; filename="cloud-config.txt"

 #cloud-config
 cloud-init directives

 --//
 Content-Type: text/x-shellscript; charset="us-ascii"
 MIME-Version: 1.0
 Content-Transfer-Encoding: 7bit
 Content-Disposition: attachment; filename="userdata.txt"

 #!/bin/bash
 shell script commands
 --//--
```

Por ejemplo, los siguientes datos de usuario incluyen las directivas cloud-init y un script de un shell bash. Las directivas cloud-init crean un archivo (`/test-cloudinit/cloud-init.txt`) y escriben `Created by cloud-init` en dicho archivo. El script de shell bash crea un archivo (`/test-userscript/userscript.txt`) y escribe `Created by bash shell script` en dicho archivo.

```
Content-Type: multipart/mixed; boundary="//"
 MIME-Version: 1.0

 --//
 Content-Type: text/cloud-config; charset="us-ascii"
 MIME-Version: 1.0
 Content-Transfer-Encoding: 7bit
 Content-Disposition: attachment; filename="cloud-config.txt"

 #cloud-config
 runcmd:
 - [ mkdir, /test-cloudinit ]
 write_files:
 - path: /test-cloudinit/cloud-init.txt
 content: Created by cloud-init

 --//
 Content-Type: text/x-shellscript; charset="us-ascii"
 MIME-Version: 1.0
 Content-Transfer-Encoding: 7bit
 Content-Disposition: attachment; filename="userdata.txt"

 #!/bin/bash
 mkdir test-userscript
 touch /test-userscript/userscript.txt
 echo "Created by bash shell script" >> /test-userscript/userscript.txt
 --//--
```

Cómo gestiona Amazon EC2 los datos de usuario de las instancias de Windows

En las instancias de Windows, los agentes de inicialización predeterminados para la versión de su sistema operativo gestionan los datos de los usuarios de la siguiente manera.

- EC2Launch v2 ejecuta scripts de datos de usuario en Windows Server 2022
- ??? ejecuta scripts de datos de usuario en Windows Server 2016 y 2019
- ??? ejecuta scripts de datos de usuario en versiones de Windows Server anteriores a Windows Server 2016

Para obtener ejemplos del ensamblado de una propiedad `UserData` en una plantilla deAWS CloudFormation, consulte Propiedad UserData cifrada en Base64 y Propiedad UserData cifrada en Base64 con AccessKey y SecretKey.

Para ver un ejemplo de ejecución de comandos en una instancia del grupo de escalado automático que funciona con enlaces de ciclo de vida, consulte el Tutorial: Configurar datos de usuario para recuperar el estado de ciclo de vida de destino a través de los metadatos de la instancia en la Guía del usuario de Amazon EC2 Auto Scaling.

Contenido

- Scripts de datos de usuario
- Ejecución de datos de usuario
- Datos de usuario y la consola
- Datos de usuario y las Tools for Windows PowerShell

Scripts de datos de usuario

Para que `EC2Config` o `EC2Launch` ejecuten scripts, debe incluir el script dentro de una etiqueta especial al agregarlo a los datos de usuario. La etiqueta que se utiliza depende de si los comandos se ejecutan en una ventana del símbolo del sistema (comandos por lotes) o con Windows PowerShell.

Si se especifica tanto un script de procesamiento por lotes como un script de Windows PowerShell, el script por lotes se ejecuta en primer lugar y después lo hace el script de Windows PowerShell, independientemente del orden en el que aparezcan en los datos de usuario de la instancia.

Si utiliza una API de AWS, incluida la AWS CLI, en un script de datos del usuario, debe utilizar un perfil de instancia al iniciar la instancia. Un perfil de instancia proporciona las credenciales de AWS adecuadas requeridas por el script de datos de usuario para ejecutar la llamada a la API. Para obtener más información, consulte Perfiles de instancias. Los permisos que asigne al rol de IAM dependen de los servicios a los que llame con la API. Para obtener más información, consulte Roles de IAM para Amazon EC2.

Tipo de script

- Sintaxis de los scripts de procesamiento por lotes
- Sintaxis de los scripts de Windows PowerShell
- Sintaxis de los scripts de configuración de YAML

- Codificación Base64

Sintaxis de los scripts de procesamiento por lotes

Especifique un script de procesamiento por lotes con la etiqueta `script`. Separe los comandos mediante saltos de línea, como se muestra en el siguiente ejemplo.

```
<script>
 echo Current date and time >> %SystemRoot%\Temp\test.log
 echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
 </script>
```

De forma predeterminada, los scripts de datos de usuario se ejecutan solo una vez, cuando se inicia la instancia. Para ejecutarlos cada vez que se inicia o se reinicia la instancia, añade `<persist>true</persist>` a los datos de usuario.

```
<script>
 echo Current date and time >> %SystemRoot%\Temp\test.log
 echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
 </script>
 <persist>true</persist>
```

Agente EC2Launch v2

Para ejecutar un script de datos de usuario XML como un proceso independiente con la tarea executeScript de EC2Launch v2 en la etapa `UserData`, agregue la siguiente etiqueta a sus datos de usuario.

`<detach>true</detach>`

> **Note**
>
> La etiqueta de desconexión no es compatible con los agentes de inicialización anteriores.

```
<script>
 echo Current date and time >> %SystemRoot%\Temp\test.log
 echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
 </script>
```

```
 <detach>true</detach>
```

Sintaxis de los scripts de Windows PowerShell

Las AMI de Windows de AWS incluyen las AWS Tools for Windows PowerShell, por lo que puede especificar estos cmdlets en los datos de usuario. Si asocia un rol de IAM a la instancia, no es necesario especificar credenciales para los cmdlets, ya que las aplicaciones que se ejecutan en la instancia pueden utilizar las credenciales del rol para obtener acceso a los recursos de AWS (por ejemplo, los buckets de Amazon S3).

Especifique un script de Windows PowerShell con la etiqueta `<powershell>`. Separe los comandos con saltos de línea. La etiqueta `<powershell>` no distingue entre mayúsculas y minúsculas.

Por ejemplo:

```
<powershell>
 $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
 New-Item $file -ItemType file
 </powershell>
```

De forma predeterminada, los scripts de datos de usuario se ejecutan solo una vez, cuando se inicia la instancia. Para ejecutarlos cada vez que se inicia o se reinicia la instancia, añade `<persist>true</persist>` a los datos de usuario.

```
<powershell>
 $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
 New-Item $file -ItemType file
 </powershell>
 <persist>true</persist>
```

Puede especificar uno o varios argumentos de PowerShell con la etiqueta `<powershellArguments>`. Si no se pasa ningún argumento, EC2Launch y EC2Launch v2 agregan el siguiente argumento de forma predeterminada: `-ExecutionPolicy Unrestricted`.

Ejemplo:

```
<powershell>
   $file = $env:SystemRoot + "\Temp" + (Get-Date).ToString("MM-dd-yy-hh-mm")
   New-Item $file -ItemType file
 </powershell>
```

```
 <powershellArguments>-ExecutionPolicy Unrestricted -NoProfile -NonInteractive</
powershellArguments>
```

Agente EC2Launch v2

Para ejecutar un script de datos de usuario XML como un proceso independiente con la tarea executeScript de EC2Launch v2 en la etapa `UserData`, agregue la siguiente etiqueta a sus datos de usuario.

```
<detach>true</detach>
```

> **Note**
>
> La etiqueta de desconexión no es compatible con los agentes de inicialización anteriores.

```
<powershell>
 $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
 New-Item $file -ItemType file
 </powershell>
 <detach>true</detach>
```

Sintaxis de los scripts de configuración de YAML

Si está utilizando EC2Launch v2 para ejecutar scripts, puede utilizar el formato YAML. Para ver tareas de configuración, detalles y ejemplos de EC2Launch v2, consulte Configuración de tareas de EC2Launch v2.

Especifique una secuencia de comandos YAML con el paso `executeScript`.

Ejemplo de sintaxis de YAML para ejecutar un script de PowerShell

```
version: 1.0
 tasks:
 - task: executeScript
   inputs:
   - frequency: always
     type: powershell
     runAs: localSystem
     content: |-
```

```
        $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
        New-Item $file -ItemType file
```

Ejemplo de sintaxis YAML para ejecutar un script por lotes

```
version: 1.1
 tasks:
 - task: executeScript
   inputs:
   - frequency: always
     type: batch
     runAs: localSystem
     content: |-
       echo Current date and time >> %SystemRoot%\Temp\test.log
       echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
```

Codificación Base64

Si utiliza Amazon EC2 API o una herramienta que no realice codificación base64 de los datos de usuario, debe codificar los datos de usuario usted mismo. De lo contrario, se registra un error por imposibilidad de encontrar etiquetas `script` o `powershell` para ejecutar. A continuación se ofrece un ejemplo de codificación con Windows PowerShell.

```
$UserData =
 [System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes($Script))
```

A continuación se ofrece un ejemplo de descodificación con PowerShell.

```
$Script =
 [System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($UserData))
```

Para obtener más información acerca de la codificación base64, consulte https://www.ietf.org/rfc/rfc4648.txt.

Ejecución de datos de usuario

De forma predeterminada, todas las AMI de Windows de AWS tienen habilitada la ejecución de datos de usuario para la inicialización inicial. Puede especificar que los scripts de datos de usuario se ejecuten la próxima vez que la instancia se inicie o reinicie. O puede especificar que los scripts de datos de usuario se ejecuten cada vez que la instancia se inicie o reinicie.

> **Note**
>
> Los datos de usuario no están habilitados para ejecutarse de forma predeterminada después de la inicialización inicial. Para permitir que los datos de usuario se ejecuten al reiniciar o iniciar la instancia, consulte Inicios o reinicios posteriores.

Los scripts de datos de usuario se ejecutan desde la cuenta del administrador local cuando se genera una contraseña aleatoria. De lo contrario, los scripts de datos de usuario se ejecutan desde la cuenta Sistema.

inicialización de la instancia

Los scripts de los datos de usuario de la instancia se ejecutan durante la inicialización inicial de la instancia. Si se encuentra la etiqueta `persist`, significa que la ejecución de los datos de usuario está habilitada para inicios o reinicios posteriores. Los archivos de registro de EC2Launch v2, EC2Launch y EC2Config contienen información del resultado estándar y las secuencias de error estándar.

EC2Launch v2

El archivo de registro de EC2Launch v2 es `C:\ProgramData\Amazon\EC2Launch\log\agent.log`.

> **Note**
>
> Es posible que la carpeta `C:\ProgramData` esté oculta. Para ver la carpeta, debe mostrar los archivos y las carpetas ocultos.

Al ejecutar los datos de usuario, se registra la información siguiente:

- `Info: Converting user-data to yaml format`: si los datos del usuario se proporcionaron en formato XML
- `Info: Initialize user-data state`: el inicio de la ejecución de datos de usuario
- `Info: Frequency is: always`: si la tarea de datos de usuario se está ejecutando en cada arranque
- `Info: Frequency is: once`: si la tarea de datos de usuario se está ejecutando una sola vez

- `Stage: postReadyUserData execution completed`: el final de la ejecución de datos de usuario

EC2Launch

El archivo de registro de EC2Launch es `C:\ProgramData\Amazon\EC2-Windows\Launch\Log\UserdataExecution.log`.

Es posible que la carpeta `C:\ProgramData` esté oculta. Para ver la carpeta, debe mostrar los archivos y las carpetas ocultos.

Al ejecutar los datos de usuario, se registra la información siguiente:

- `Userdata execution begins`: el inicio de la ejecución de datos de usuario
- `<persist> tag was provided: true`: si se encuentra la etiqueta persistir
- `Running userdata on every boot`: si se encuentra la etiqueta persistir
- `<powershell> tag was provided.. running powershell content`: si se encuentra la etiqueta powershell
- `<script> tag was provided.. running script content`: si se encuentra la etiqueta script
- `Message: The output from user scripts`: si se ejecutan scripts de datos de usuario, se registra su salida

EC2Config

El archivo de registro de EC2Config es `C:\Program Files\Amazon\Ec2ConfigService\Logs\Ec2Config.log`. Al ejecutar los datos de usuario, se registra la información siguiente:

- `Ec2HandleUserData: Message: Start running user scripts`: el inicio de la ejecución de datos de usuario
- `Ec2HandleUserData: Message: Re-enabled userdata execution`: si se encuentra la etiqueta persistir
- `Ec2HandleUserData: Message: Could not find <persist> and </persist>`: si no se encuentra la etiqueta persistir
- `Ec2HandleUserData: Message: The output from user scripts`: si se ejecutan scripts de datos de usuario, se registra su salida

Inicios o reinicios posteriores

Cuando se actualizan los datos de usuario de la instancia, los scripts de datos de usuario no se ejecutan automáticamente al iniciar o reiniciar la instancia. Sin embargo, puede habilitar la ejecución de los datos de usuario para que los scripts que los contienen se ejecuten una sola vez al iniciar o reiniciar la instancia, o bien cada vez que esta se inicie o se reinicie.

Si elige la opción Cerrar con Sysprep, los scripts de datos de usuario se ejecutarán la próxima vez que comience o se reinicie la instancia, aunque no se haya habilitado la ejecución de los datos de usuario para comienzos o reinicios posteriores. Los scripts de datos de usuario no se ejecutarán en reinicios o comienzos posteriores.

Habilitar la ejecución de datos de usuario con EC2Launch v2 (Vista previa de las AMI)

- Ejecutar una tarea en los datos de usuario en el primer arranque, establezca `frequency` en `once`.
- Ejecutar una tarea en los datos de usuario en cada arranque, establezca `frequency` en `always`.

Habilitar la ejecución de datos de usuario en Windows Server 2016 o versiones posteriores (EC2Launch)

1. Conéctese a la instancia de Windows.
2. Abra una ventana de comandos de PowerShell y ejecute el comando siguiente:

   ```
   C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -Schedule
   ```

3. Desconéctese de la instancia de Windows. Para ejecutar los scripts actualizados la próxima vez que se inicie la instancia, detén la instancia y actualiza los datos de usuario.

Habilitar la ejecución de datos de usuario en Windows Server 2012 EC2Config y versiones anteriores (R2)

1. Conéctese a la instancia de Windows.
2. Abrir `C:\Program Files\Amazon\Ec2ConfigService\Ec2ConfigServiceSetting.exe`.
3. En User Data (Datos de usuario), seleccione Enable UserData execution for next service start (Habilitar la ejecución de datos de usuario en el siguiente inicio de servicio).
4. Desconéctese de la instancia de Windows. Para ejecutar los scripts actualizados la próxima vez que se inicie la instancia, detén la instancia y actualiza los datos de usuario.

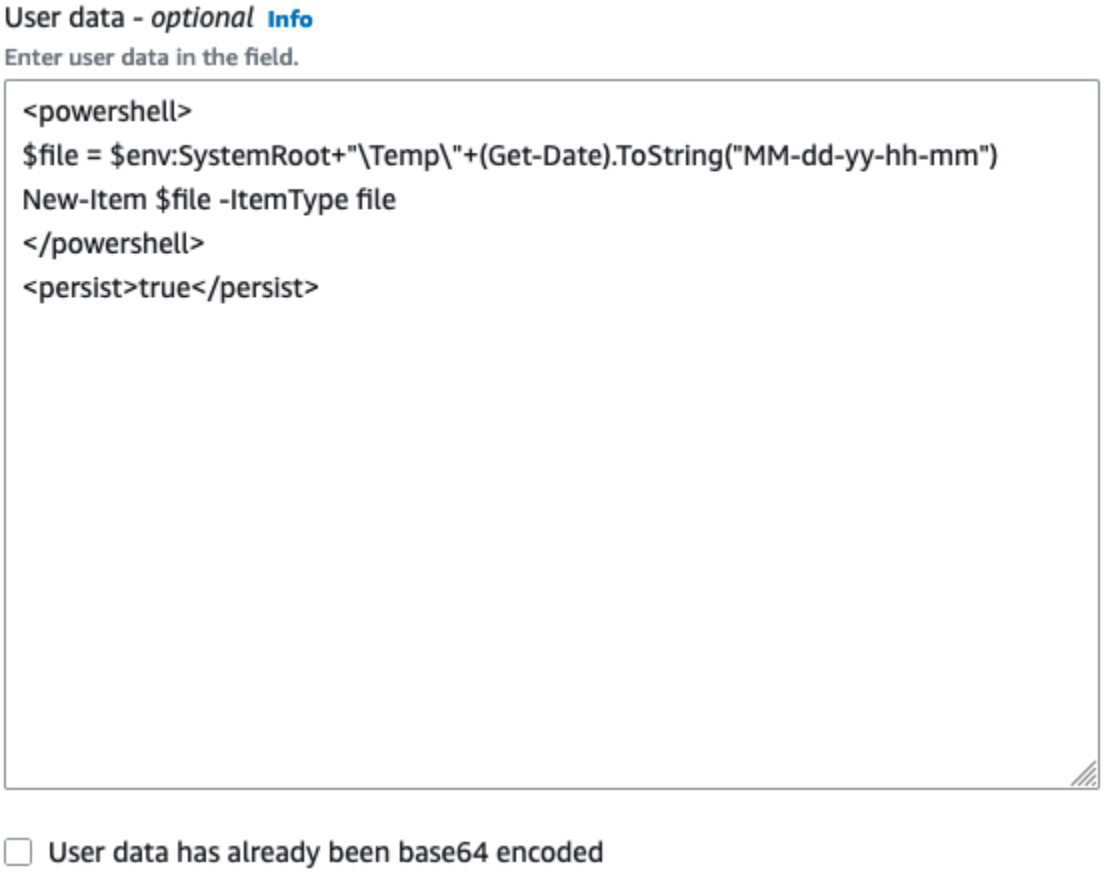
Datos de usuario y la consola

Puede especificar los datos de usuario de la instancia al iniciar la instancia. Si el volumen raíz de la instancia es un volumen de EBS, también puede detener la instancia y actualizar los datos de usuario.

Especificar los datos de usuario de la instancia durante la inicialización

Siga el procedimiento para iniciar una instancia. El campo User data (Datos de usuario) se encuentra en la sección Detalles avanzados del asistente de inicialización de instancias. Ingrese el script de shell en el campo User data y, a continuación, complete el procedimiento de inicialización de instancias.

En la siguiente captura de pantalla del campo de datos del usuario, la secuencia de comandos de ejemplo crea un archivo en la carpeta temporal de Windows, utilizando la fecha y la hora actuales en el nombre del archivo. Al incluir `<persist>true</persist>`, el script se ejecuta cada vez que comienzas o reinicias la instancia. Si deja vacía la casilla Los datos del usuario ya están codificados en base64, la consola Amazon EC2 realizará la codificación en base64 por usted.



Visualizar y actualizar los datos de usuario de la instancia

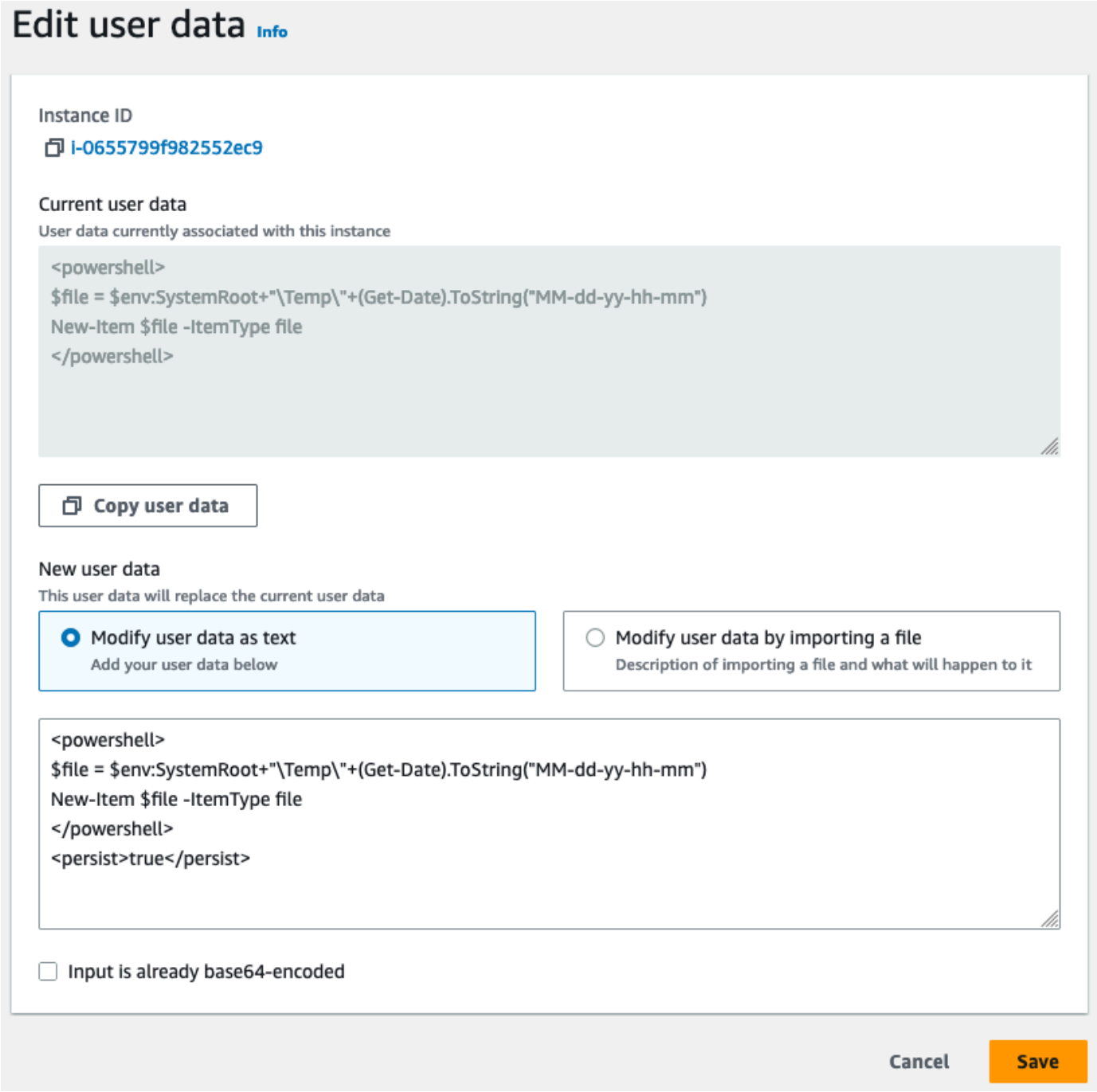
Puede ver los datos de usuario de cualquier instancia y actualizarlos en las instancias detenidas.

Para actualizar los datos de usuario de una instancia con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancias).
3. Seleccione la instancia y elija Actions (Acciones), Instance State (Estado de la instancia) y Stop instance (Detener instancia).

   > **Warning**
   >
   > Cuando detiene una instancia, se borran los datos contenidos en todos los volúmenes de almacén de instancias. Para conservar los datos de los volúmenes del almacén de instancias, asegúrese de realizar una copia de seguridad de ellos en un almacenamiento persistente.

4. Cuando se le pida que confirme, elija Stop. Puede que transcurran unos minutos hasta que la instancia se detenga.
5. Con la instancia aún seleccionada, elija Actions (Acciones), Instance Settings (Configuración de la instancia) y Edit user data (Editar datos del usuario). Los datos de usuario no se pueden cambiar si la instancia se está ejecutando, pero puede verlos.
6. En el cuadro de diálogo Modificar datos del usuario, actualiza los datos de usuario y a continuación selecciona Guardar. Para ejecutar los scripts de datos de usuario cada vez que comienzas o reinicias la instancia, agrega `<persist>true</persist>`, tal como se muestra en el siguiente ejemplo:



7. Inicie la instancia. Si habilitaste la ejecución de los datos de usuario para arranques o reinicios posteriores, los scripts de datos de usuario actualizados se ejecutan como parte del proceso de inicio de la instancia.

Datos de usuario y las Tools for Windows PowerShell

Puede usar la Tools for Windows PowerShell para especificar, modificar y ver los datos de usuario de la instancia. Para obtener más información acerca de cómo ver los datos de usuario de la instancia usando los metadatos de la instancia, consulte Recuperación de los datos de usuario de la instancia desde su instancia. Para obtener más información sobre datos de usuario y AWS CLI, consulte Datos de usuario y las AWS CLI.

Ejemplo: Especificar los datos de usuario de la instancia durante la inicialización

Cree un archivo de texto con los datos de usuario de la instancia. Para ejecutar los scripts de datos de usuario cada vez que arrrancas o reinicias la instancia, agrega `<persist>true</persist>`, tal como se muestra en el siguiente ejemplo.

```
<powershell>
 $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
 New-Item $file -ItemType file
 </powershell>
 <persist>true</persist>
```

Para especificar los datos de usuario de la instancia cuando inicia la instancia, use el comando New-EC2Instance. Este comando no realiza codificación base64 de los datos de usuario. Para codificar los datos de usuario en un archivo de texto llamado `script.txt`, utilice los siguientes comando.

```
PS C:\> $Script = Get-Content -Raw script.txt
 PS C:\> $UserData =
 [System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes($Script))
```

Utilice el parámetro `-UserData` para pasar los datos de usuario al comando New-EC2Instance.

```
PS C:\> New-EC2Instance -ImageId ami-abcd1234 -MinCount 1 -MaxCount 1 -
InstanceType m3.medium \
 -KeyName my-key-pair -SubnetId subnet-12345678 -SecurityGroupIds sg-1a2b3c4d \
 -UserData $UserData
```

Ejemplo: Actualizar los datos de usuario de una instancia detenida

Puede modificar los datos de usuario de una instancia detenida utilizando el comando Edit-EC2InstanceAttribute.

Cree un archivo de texto con el nuevo script. Para codificar los datos de usuario en el archivo de texto llamado `new-script.txt`, utilice los siguientes comando.

```
PS C:\> $NewScript = Get-Content -Raw new-script.txt
 PS C:\> $NewUserData =
 [System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes($NewScript))
```

Utilice los parámetros `-UserData` y `-Value` para especificar los datos de usuario.

```
PS C:\> Edit-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -Attribute userData -
Value $NewUserData
```

Ejemplo: Ver los datos de usuario de la instancia

Para recuperar los datos de usuario de una instancia, utilice el comando Get-EC2InstanceAttribute.

```
PS C:\> (Get-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -Attribute
 userData).UserData
```

A continuación, se muestra un ejemplo del resultado. Tenga en cuenta que los datos de usuario están codificados.

```
PHBvd2Vyc2hlbGw
+DQpSZW5hbWUtQ29tcHV0ZXIgLU5ld05hbWUgdXNlci1kYXRhLXRlc3QNCjwvcG93ZXJzaGVsbD4=
```

Para almacenar los datos de usuario codificados en una variable y luego decodificarlos, utilice los siguientes comandos.

```
PS C:\> $UserData_encoded = (Get-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -
Attribute userData).UserData
 PS C:
\> [System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($UserData_encoded)
```

A continuación, se muestra un ejemplo del resultado.

```
<powershell>
 $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
 New-Item $file -ItemType file
 </powershell>
 <persist>true</persist>
```

Ejemplo: Cambiar el nombre a la instancia para que coincida con el valor de la etiqueta

Puede utilizar el comando Get-EC2Tag para leer el valor de la etiqueta, cambiar el nombre a la instancia durante el primer arranque para que coincida con el valor de la etiqueta y reiniciar. Para ejecutar este comando correctamente, debe tener un rol con permisos `ec2:DescribeTags` adjunto a la instancia, porque la información de etiquetas se recupera mediante una llamada a la API. Para obtener más información acerca de los permisos de configuración mediante roles de IAM, consulte Asociar un rol de IAM a una instancia.

> **Note**
>
> Este script falla en versiones de Windows Server anteriores a 2008.

```
<powershell>
 $instanceId = (invoke-webrequest http://169.254.169.254/latest/meta-data/instance-id -
UseBasicParsing).content
 $nameValue = (get-ec2tag -filter @{Name="resource-id";Value=
$instanceid},@{Name="key";Value="Name"}).Value
 $pattern = "^(?![0-9]{1,15}$)[a-zA-Z0-9-]{1,15}$"
 #Verify Name Value satisfies best practices for Windows hostnames
 If ($nameValue -match $pattern)
     {Try
         {Rename-Computer -NewName $nameValue -Restart -ErrorAction Stop}
     Catch
         {$ErrorMessage = $_.Exception.Message
         Write-Output "Rename failed: $ErrorMessage"}}
 Else
     {Throw "Provided name not a valid hostname. Please ensure Name value is between 1
 and 15 characters in length and contains only alphanumeric or hyphen characters"}
 </powershell>
```

También puede cambiar el nombre de la instancia mediante etiquetas en los metadatos de la instancia, si la instancia está configurada para etiquetas de acceso desde los metadatos de instancia. Para obtener más información, consulte Trabajar con etiquetas de instancia en los metadatos de instancia.

> **Note**
>
> Este script falla en versiones de Windows Server anteriores a 2008.

```
<powershell>
 $nameValue = Get-EC2InstanceMetadata -Path /tags/instance/Name
 $pattern = "^(?![0-9]{1,15}$)[a-zA-Z0-9-]{1,15}$"
 #Verify Name Value satisfies best practices for Windows hostnames
 If ($nameValue -match $pattern)
     {Try
         {Rename-Computer -NewName $nameValue -Restart -ErrorAction Stop}
     Catch
         {$ErrorMessage = $_.Exception.Message
         Write-Output "Rename failed: $ErrorMessage"}}
 Else
     {Throw "Provided name not a valid hostname. Please ensure Name value is between 1
 and 15 characters in length and contains only alphanumeric or hyphen characters"}
 </powershell>
```

Conexión con instancias EC2

En esta sección de la Guía del usuario de Amazon EC2 se proporciona información para que pueda conectarse a la instancia de Amazon EC2 después de iniciarla. También proporciona información para ayudarlo a conectar la instancia a otro recurso de AWS.

Temas

- Conexión con la instancia de Linux
- Conexión con la instancia de Windows de
- Conexión mediante el Administrador de sesiones
- Conexión a las instancias mediante el punto de conexión de EC2 Instance Connect
- Conexión de una instancia de EC2 a un recurso de AWS

Conexión con la instancia de Linux

Existen diversas maneras de conectarse a su instancia Linux. Algunas varían según el sistema operativo del equipo local desde el que se conecte. Otras, como EC2 Instance Connect o Session Manager de AWS Systems Manager, no varían. En esta sección, puede aprender cómo conectar su instancia de Linux y cómo transferir archivos entre su equipo local y su instancia.

Antes de conectarse a la instancia de Linux, debe completar los siguientes requisitos previos.

- Obtenga información sobre su instancia

- Busque la clave privada y establezca permisos.
- (Opcional) Obtenga la huella digital de la instancia

A continuación, elija una de las siguientes opciones para conectarse a su instancia de Linux.

Opciones para conectarse en función de su sistema operativo local

- Conéctese desde una máquina local Linux o macOS mediante SSH
- Conéctese desde un equipo local de Windows

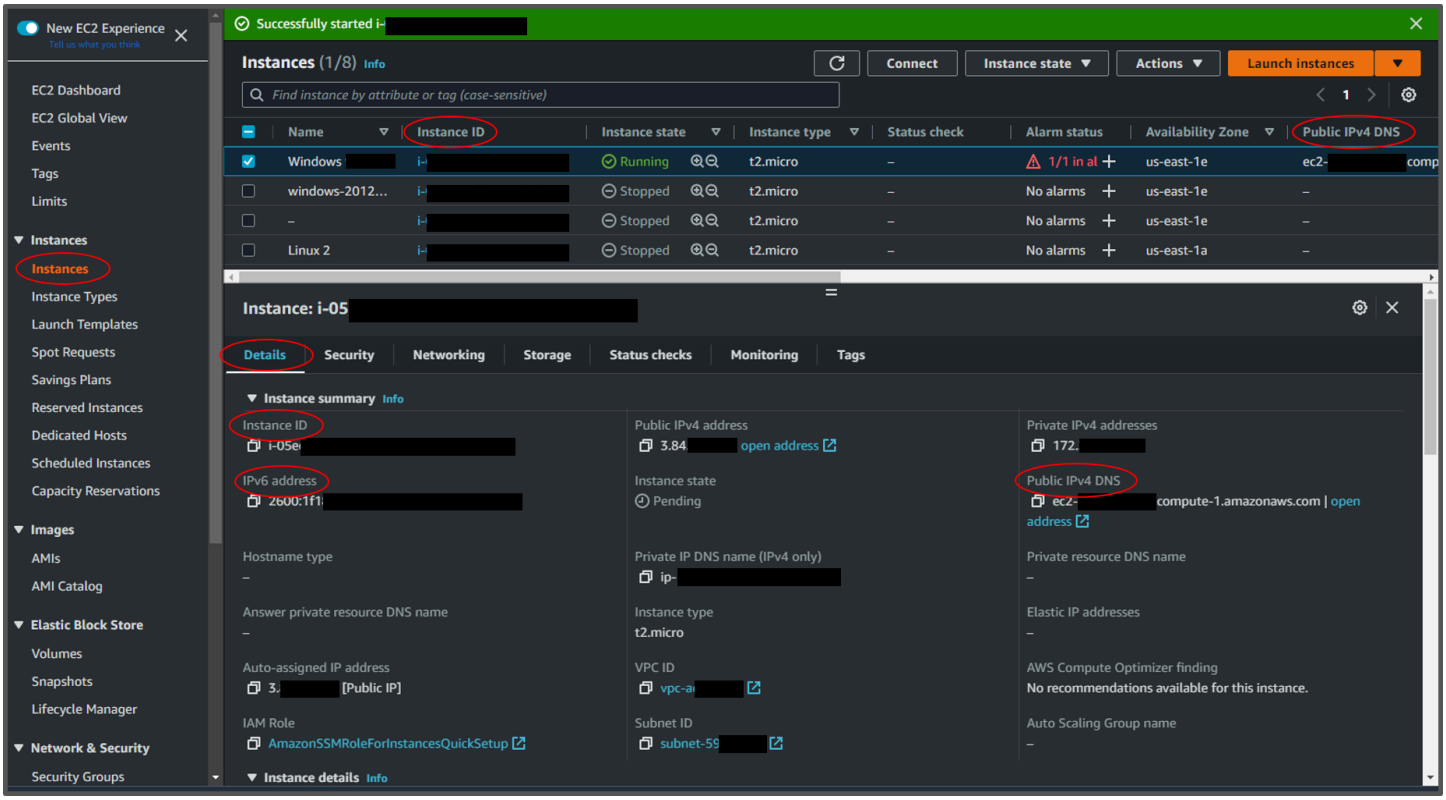
Opciones para conectarse desde cualquier sistema operativo local

- Conexión mediante el Administrador de sesiones
- Conéctese a la instancia de Linux con EC2 Instance Connect.

> **Note**
>
> Para obtener sugerencias para solucionar problemas de conexión de instancias, consulte Solución de problemas de conexión a la instancia de Linux.
> Para solucionar problemas de arranque, configuración de red y otros problemas para las instancias creadas en el Sistema Nitro de AWS, puede usar Consola serie de EC2 para instancias de Amazon EC2.

Obtenga información sobre su instancia

Para prepararse para conectarse a una instancia, obtenga la siguiente información en la consola de Amazon EC2 o mediante la AWS CLI.



- Obtenga el nombre de DNS público de la instancia.

  Puede obtener el DNS público para su instancia de la consola de Amazon EC2. Compruebe la columna DNS de IPv4 público del panel instancias. Si esta columna está oculta, elija el icono de configuración ( ) en la esquina superior derecha de la pantalla y seleccione DNS de IPv4 público. También puede encontrar el DNS público en la sección de información de instancias del panel instancias. Al seleccionar la instancia en el panel instancias de la consola de Amazon EC2, la información sobre esa instancia aparecerá en la mitad inferior de la página. En la pestaña Detalles, busque DNS de IPv4 público.

  Si lo prefiere, puede usar los comandos Describir instancias (AWS CLI) o el comando Obtener instancia de EC2 (AWS Tools for Windows PowerShell).

  Si no se muestra ningún DNS de IPv4 público, compruebe que el estado de la instancia esté en ejecución y que no la haya iniciado en una subred privada. Si lanzó la instancia mediante el asistente de inicialización de instancias, es posible que haya editado el campo Asignar automáticamente IP pública en Configuración de red y haya modificado el valor a Deshabilitar.

Si deshabilita la opción Asignar automáticamente IP pública, a la instancia no se le asignará una dirección IP pública cuando se lance.

- (Solo IPv6) Obtenga la dirección IPv6 de la instancia.

  Si asignó una dirección IPv6 a la instancia, puede conectarse opcionalmente a la instancia con su dirección IPv6, en lugar de con una dirección IPv4 pública o un nombre de host DNS IPv4 público. El equipo local debe tener una dirección IPv6 y estar configurado para usar IPv6. Puede obtener la dirección IPv6 para su instancia de la consola de Amazon EC2. Consulte la columna IP de IPv6 del panel instancias. O bien, puede encontrar la dirección IPv6 en la sección de información de la instancia. Al seleccionar la instancia en el panel instancias de la consola de Amazon EC2, la información sobre esa instancia aparecerá en la mitad inferior de la página. En la pestaña Detalles, busque la dirección IPv6.

  Si lo prefiere, puede usar los comandos Describir instancias (AWS CLI) o el comando Obtener instancia de EC2 (AWS Tools for Windows PowerShell). Para obtener información sobre IPv6, consulte Direcciones IPv6.

- Obtener el nombre de usuario de su instancia.

  Puede conectarse a la instancia mediante el nombre de usuario de su cuenta de usuario o el nombre de usuario predeterminado de la AMI que utilizó para iniciar la instancia.

  - Obtener el nombre de usuario de su cuenta de usuario.

    Para obtener más información sobre cómo crear una cuenta de usuario, consulte Administración de usuarios del sistema en la instancia de Linux.

  - Obtenga el nombre de usuario predeterminado para la AMI que utilizó para iniciar la instancia:

AMI utilizada para iniciar la instancia.	Nombre de usuario predeterminado
AL2023 Amazon Linux 2 Amazon Linux	`ec2-user`
CentOS	`centos` o `ec2-user`
Debian	`admin`

AMI utilizada para iniciar la instancia.	Nombre de usuario predeterminado
Fedora	`fedora` o `ec2-user`
RHEL	`ec2-user` o `root`
SUSE	`ec2-user` o `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`
Rocky Linux	`rocky`
Otro	Comprobación con el proveedor de AMI

Busque la clave privada y establezca permisos.

Debe conocer la ubicación del archivo de clave privada para conectarse a la instancia. Para las conexiones SSH, debe establecer los permisos para que solo usted pueda leer el archivo.

Para obtener información sobre cómo funcionan los pares de claves cuando se utiliza Amazon EC2, consulte Pares de claves e instancias de Amazon EC2.

- Busque la clave privada

  Obtenga la ruta completa de la ubicación del archivo `.pem` en su equipo con el par de claves que especificó cuando lanzó la instancia. Para obtener más información, consulte the section called “Identificación del par de claves públicas que se especificó en el lanzamiento”.

  Si no encuentra el archivo de clave privada, consulte

  > Si pierde la clave privada para una instancia respaldada por EBS, puede volver a obtener acceso a la instancia. Para ello, debe detener la instancia, desconectar su volumen raíz y asociarlo a otra instancia como volumen de datos, modificar el archivo `authorized_keys` con una nueva clave pública, trasladar el volumen de nuevo a la instancia original y reiniciar la instancia. Para obtener más información acerca de cómo lanzar, conectar y detener instancias, consulte Ciclo de vida de la instancia.

Este procedimiento solo se admite para instancias con volúmenes raíz de EBS. Si el dispositivo raíz es un volumen del almacén de instancias, no puede utilizar este procedimiento para recuperar el acceso a la instancia; debe tener la clave privada para conectarse a la instancia. Para determinar el tipo de dispositivo raíz de la instancia, abra la consola de Amazon EC2, elija Instancias, seleccione la instancia, elija la pestaña Almacenamiento y, en la sección Detalles del dispositivo raíz compruebe el valor de Tipo de dispositivo raíz.

El valor es `EBS` o `INSTANCE-STORE`.

Además de los siguientes pasos, hay otras formas de conectarse a la instancia de Linux si extravía la clave privada. Para obtener más información, consulte ¿Cómo puedo conectarme a mi instancia de Amazon EC2 si he extraviado mi par de claves SSH después del lanzamiento inicial?

Pasos para conectarse a una instancia respaldada por EBS con un par de claves diferente

Paso 1: Crear un nuevo par de claves

Cree un nuevo par de claves mediante la consola de Amazon EC2 o una herramienta de terceros. Si desea dar al nuevo par de claves el mismo nombre que tenía la clave privada que perdió, primero debe eliminar el par de claves existente. Para obtener información sobre cómo crear un par de claves, consulte Crear un par de claves mediante Amazon EC2 o Crear un par de claves con una herramienta de terceros e importar la clave pública a Amazon EC2.

Paso 2: Obtener información sobre la instancia original y su volumen raíz

Tome nota de la siguiente información porque la necesitará para completar este procedimiento.

Para obtener información sobre la instancia original

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. Elija Instances (Instancias) en el panel de navegación y, a continuación, seleccione la instancia a la que desee conectarse. (Nos referiremos a ella como la instancia original).
3. En la pestaña Details (Detalles), tome nota del ID de la instancia y del ID de la AMI.
4. En la pestaña Networking (Redes), tome nota de la zona de disponibilidad.
5. En la pestaña Storage (Almacenamiento), en Root device name (Nombre del dispositivo raíz), tome nota del nombre del dispositivo para el volumen raíz (por ejemplo, `/dev/xvda`).

   A continuación, en Block devices (Dispositivos de bloqueo), busque el nombre de este dispositivo y tome nota del ID del volumen (por ejemplo, vol-0a1234b5678c910de).

Paso 3: Detener la instancia original

Elija Instance state (Estado de la instancia) y Stop instance (Detener instancia). Si esta opción está desactivada, la instancia ya está detenida o bien su dispositivo raíz es un volumen de almacén de instancias.

> **Warning**
>
> Cuando detiene una instancia, se borran los datos contenidos en todos los volúmenes de almacén de instancias. Para conservar los datos de los volúmenes del almacén de instancias, asegúrese de realizar una copia de seguridad de ellos en un almacenamiento persistente.

Paso 4: Lanzar una instancia temporal

New console

Para iniciar una instancia temporal

1. En el panel de navegación, elija Instances (Instancias) y, a continuación, Launch Instances (Lanzar instancias).
2. En la sección Name and tags (Nobre y etiquetas), para Name (Nombre), ingrese Temporary (Provisorio).
3. En la sección Application and OS Images (Imágenes de aplicaciones y SO), seleccione la misma AMI que utilizó para lanzar la instancia original. Si esta AMI no está disponible, puede crear una AMI que puede utilizar a partir de la instancia detenida. Para obtener más información, consulte Creación de una AMI basada en Amazon EBS.
4. En la sección Instance type (Tipo de instancia), mantenga el tipo de instancia predeterminado.
5. En la sección Key pair (Par de claves), para Key pair name (Nombre del par de claves), seleccione el par de claves existente para utilizar o crear uno nuevo.
6. En la sección Network settings (Configuración de red), elija Edit (Editar) y, a continuación, para Subnet (Subred), seleccione una subred en la misma zona de disponibilidad que la instancia original.
7. En el panel Summary (Resumen), elija Launch (Lanzar).

Old console

Elija Launch Instances (Lanzar instancias) y, a continuación, utilice el launch wizard para lanzar una instancia temporal con las siguientes opciones:

- En la página Choose an AMI (Elegir una AMI), seleccione la misma AMI que utilizó para lanzar la instancia original. Si esta AMI no está disponible, puede crear una AMI que puede utilizar a partir de la instancia detenida. Para obtener más información, consulte Creación de una AMI basada en Amazon EBS.
- En la página Choose an Instance Type (Elegir un tipo de instancia), deje el tipo de instancia predeterminado que el asistente haya seleccionado.

- En la página Configure Instance Details (Configurar detalles de instancia), especifique la misma zona de disponibilidad que la de la instancia original. Si va a lanzar una instancia en una VPC, seleccione una subred en esta zona de disponibilidad.
- En la página Add Tags (Añadir etiquetas), añada la etiqueta `Name=Temporary` a la instancia para indicar que se trata de una instancia temporal.
- En la página Review (Revisión), seleccione Launch (Lanzar). Elija el par de claves que creó en el paso 1 y, a continuación, elija Launch Instances (Lanzar instancias).

Paso 5: Desconectar el volumen raíz de la instancia original y asociarlo a la instancia temporal

1. En el panel de navegación, elija Volumes (Volúmenes) y seleccione el volumen de dispositivo raíz para la instancia original (tomó nota del ID de su volumen en uno paso previo). Elija Actions (Acciones), Detach volume (Desconectar volumen) y, luego, Detach (Desconectar). Espere a que el estado del volumen cambie a `available`. (Es posible que necesite seleccionar el icono Actualizar).
2. Con el volumen todavía seleccionado, elija Actions (Acciones) y, a continuación, elija Attach Volume (Adjuntar volumen). Seleccione el ID de la instancia temporal, tome nota del nombre del dispositivo especificado en Device name (Nombre del dispositivo) (por ejemplo, `/dev/sdf`) y, a continuación, elija Attach volume (Adjuntar volumen).

> **Note**
>
> Si lanzó la instancia original a partir de una AMI de AWS Marketplace y el volumen contiene códigos de AWS Marketplace, primero debe detener la instancia temporal antes de poder adjuntar el volumen.

Paso 6: Agregar la nueva clave pública a **`authorized_keys`** en el volumen original montado en la instancia temporal

1. Conéctese a la instancia temporal.
2. Desde la instancia temporal, monte el volumen que adjuntó a la instancia para que pueda obtener acceso a su sistema de archivos. Por ejemplo, si el nombre de dispositivo es `/dev/sdf`, utilice los siguientes comandos para montar el volumen como `/mnt/tempvol`.

> **Note**
>
> El nombre de dispositivo podría aparecer de forma diferente en la instancia. Por ejemplo, los dispositivos montados como `/dev/sdf` podrían mostrarse como `/dev/xvdf` en la instancia. Algunas versiones de Red Hat (o sus variantes como CentOS), incluso pueden aumentar la letra final en cuatro caracteres, donde `/dev/sdf` se convierte en `/dev/xvdk`.

a. Utilice el comando lsblk para determinar si el volumen está particionado.

```
[ec2-user ~]$ lsblk
NAME    MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda    202:0    0    8G  0 disk
##xvda1 202:1    0    8G  0 part /
xvdf    202:80   0  101G  0 disk
##xvdf1 202:81   0  101G  0 part
xvdg    202:96   0   30G  0 disk
```

En el ejemplo anterior, `/dev/xvda` y `/dev/xvdf` son volúmenes particionados, mientras que `/dev/xvdg` no lo es. Si el volumen está particionado, monte la partición (`/dev/xvdf1`) en lugar del dispositivo tal cual (`/dev/xvdf`) en los siguientes pasos.

b. Cree un directorio temporal para montar el volumen.

```
[ec2-user ~]$ sudo mkdir /mnt/tempvol
```

c. Monte el volumen (o la partición) en el punto de montaje temporal utilizando el nombre del volumen o el nombre de dispositivo que identificó anteriormente. El comando requerido depende del sistema de archivos de su sistema operativo. Tenga en cuenta que el nombre de dispositivo puede aparecer de forma diferente en la instancia. Consulte note en el paso 6 para más información.

- Amazon Linux, Ubuntu y Debian

```
[ec2-user ~]$ sudo mount /dev/xvdf1 /mnt/tempvol
```

- Amazon Linux 2, CentOS, SUSE Linux 12 y RHEL 7.x

```
[ec2-user ~]$ sudo mount -o nouuid /dev/xvdf1 /mnt/tempvol
```

> **Note**
>
> Si recibe un error que indica que el sistema de archivos está corrupto, ejecute el comando siguiente para usar la utilidad fsck para comprobar el sistema de archivos y reparar cualquier problema:
>
> ```
> [ec2-user ~]$ sudo fsck /dev/xvdf1
> ```

3. Desde la instancia temporal, utilice el siguiente comando para actualizar `authorized_keys` en el volumen montado con la nueva clave pública de `authorized_keys` para la instancia temporal.

> **Important**
>
> Los ejemplos siguientes utilizan el nombre de usuario de Amazon Linux `ec2-user`. Es posible que necesite sustituirlo por un nombre de usuario diferente, como `ubuntu` para las instancias de Ubuntu.

```
[ec2-user ~]$ cp .ssh/authorized_keys /mnt/tempvol/home/ec2-user/.ssh/
authorized_keys
```

Si esta copia funciona correctamente, puede proceder al paso siguiente.

(Opcional) De lo contrario, si no tiene permiso para editar archivos en `/mnt/tempvol`, debe actualizar el archivo mediante el comando sudo y, a continuación, comprobar los permisos del archivo para asegurarse de que podrá iniciar sesión en la instancia original. Use el siguiente comando para comprobar los permisos del archivo.

```
[ec2-user ~]$ sudo ls -l /mnt/tempvol/home/ec2-user/.ssh
total 4
-rw------- 1 222 500 398 Sep 13 22:54 authorized_keys
```

En el resultado de este ejemplo, *222* es el ID de usuario y *500* es el ID de grupo. A continuación, utilice el comando sudo para volver a ejecutar el comando de copia que produjo un error.

```
[ec2-user ~]$ sudo cp .ssh/authorized_keys /mnt/tempvol/home/ec2-user/.ssh/
authorized_keys
```

Ejecute el siguiente comando de nuevo para determinar si los permisos han cambiado.

```
[ec2-user ~]$ sudo ls -l /mnt/tempvol/home/ec2-user/.ssh
```

Si el ID de usuario y el ID de grupo han cambiado, use el siguiente comando para restaurarlos.

```
[ec2-user ~]$ sudo chown 222:500 /mnt/tempvol/home/ec2-user/.ssh/
authorized_keys
```

Paso 7: Desmontar y desconectar el volumen original de la instancia temporal y volver a asociarlo a la instancia original

1. Desde la instancia temporal, desmonte el volumen que adjuntó para que pueda volver a adjuntarlo a la instancia original. Por ejemplo, utilice el siguiente comando para desmontar el volumen en `/mnt/tempvol`.

   ```
   [ec2-user ~]$ sudo umount /mnt/tempvol
   ```

2. Desconecte el volumen de la instancia temporal (lo desmontó en el paso anterior): en la consola de Amazon EC2 elija Volumes (Volúmenes) en el panel de navegación, seleccione el volumen del dispositivo raíz de la instancia original (tomó nota del ID del volumen en un paso anterior), elija Actions (Acciones), Detach volume (Desconectar volumen) y, luego, Detach (Desconectar). Espere a que el estado del volumen cambie a `available`. (Es posible que necesite seleccionar el icono Refresh (Actualizar)).
3. Vuelva a conectar el volumen a la instancia original: con el volumen seleccionado, elija Actions (Acciones), Attach Volume (Adjuntar volumen). Seleccione el ID de la instancia original, especifique el nombre de dispositivo que anotó anteriormente en el paso 2 para

el adjunto del dispositivo raíz original (`/dev/sda1` o `/dev/xvda`) y, a continuación, elija Attach volume (Adjuntar volumen).

> **Important**
>
> Si no especifica el mismo nombre de dispositivo que el de la asociación original, no podrá comenzar la instancia original. Amazon EC2 espera que el volumen de dispositivo raíz sea `sda1` o `/dev/xvda`.

Paso 8: Conectarse a la instancia original utilizando el nuevo par de claves

Seleccione la instancia original y elija Instance state (Estado de la instancia) y Start instance (Iniciar instancia). Cuando la instancia pase a estado `running`, puede conectarse a ella utilizando el archivo de clave privada para su nuevo par de claves.

> **Note**
>
> Si el nombre de su nuevo par de claves y del archivo de clave privada correspondiente es diferente al del par de claves original, asegúrese de especificar el nombre del nuevo archivo de clave privada al conectarse a la instancia.

Paso 9: Limpieza

(Opcional) Puede terminar la instancia temporal cuando no vaya a utilizarla más. Seleccione la instancia temporal y elija Instance state (Estado de la instancia) y Terminate instance (Terminar instancia).

Si se conecta a la instancia mediante Putty y necesita convertir el archivo `.pem` a `.ppk`, consulte Convierta su clave privada utilizando PuTTYgen en el tema Conéctese a la instancia de Linux desde Windows con PuTTY de esta sección.

- Configure los permisos del archivo de clave privada para que solo usted pueda leerlo.
  - Conectarse desde macOS o Linux

    (Instancias de Linux) Si tiene planeado usar un cliente SSH en un equipo macOS o Linux para conectarse a su instancia de Linux, utilice el comando a continuación para establecer los permisos de su archivo de clave privada de manera que solo usted pueda leerlo.

```
chmod 400 key-pair-name.pem
```

Si no configura estos permisos, no podrá conectarse a la instancia con este par de claves. Para obtener más información, consulte Error: Unprotected Private Key File (Error: archivo de clave privada no protegido).

- Conectarse desde Windows

  Abra el Explorador de archivos y haz clic con el botón derecho en el archivo `.pem`. Seleccione la Propiedades > pestaña Seguridad y elija Avanzado. Elija Deshabilitar la herencia. Elimine el acceso a todos los usuarios excepto al usuario actual.

(Opcional) Obtenga la huella digital de la instancia

Si desea protegerse de ataques de tipo “Man in the middle”, puede verificar la huella dactilar que se muestra para comprobar la autenticidad de la instancia a la que está a punto de conectarse. La verificación de la huella dactilar es útil si lanzó la instancia desde una AMI pública proporcionada por un tercero.

Descripción general de las tareas

En primer lugar, obtenga la huella dactilar de la instancia. A continuación, cuando se conecte a la instancia y se le solicite que verifique la huella dactilar, compare la huella dactilar obtenida en este procedimiento con la huella dactilar que se muestra. Si las huellas digitales no coinciden, alguien podría intentar un ataque de intermediario. Si coinciden, puede conectarse con confianza a la instancia.

Requisitos previos necesarios para obtener la huella digital de la instancia

- La instancia no debe tener el estado `pending`. La huella digital solo está disponible después de que se haya completado el primer arranque de la instancia.
- Debe ser el propietario de la instancia para obtener la salida de la consola.
- Hay varias formas de obtener la huella dactilar de la instancia. Si desea utilizar la AWS CLI, debe estar instalada en el equipo local. Para obtener información sobre la instalación o actualización de AWS CLI, consulte Instalar AWS Command Line Interface en la Guía del usuario de AWS Command Line Interface.

Para obtener la huella digital de la instancia

En el paso 1, obtiene la salida de la consola, que incluye la huella dactilar de la instancia. En el paso 2, busca la huella dactilar de la instancia en la salida de la consola.

1. Obtenga la salida de la consola con uno de los siguientes métodos.

   Console

   1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
   2. En el navegador izquierdo, elija instancias.
   3. Seleccione su instancia y luego elija Acciones, Monitoreo y solución problemas, Obtener registro del sistema.

   AWS CLI

   En su equipo local (no en la instancia a la que se está conectando), utilice el comando get-console-output (AWS CLI). Si la salida es grande, puede canalizarla a un archivo de texto donde sea más fácil de leer. Tenga en cuenta que cuando use la AWS CLI, debe especificar una región de Región de AWS, ya sea de forma explícita o estableciendo una región predeterminada. Para obtener información sobre cómo configurar o especificar una región, consulte Conceptos básicos de configuración en la Guía del usuario de AWS Command Line Interface.

   ```
   aws ec2 get-console-output --instance-id instance_id --query Output --output
    text > temp.txt
   ```

2. En la salida de la consola, busque la huella dactilar de la instancia (host), que se encuentra en `BEGIN SSH HOST KEY FINGERPRINTS`. Puede haber varias huellas dactilares de instancia. Cuando se conecte a su instancia, se mostrará solo una de las huellas dactilares.

   El resultado exacto puede variar según el sistema operativo, la versión de AMI y si ha hecho que AWS cree los pares de claves. A continuación, se muestra un ejemplo del resultado.

   ```
   ec2:#############################################################
   ec2: -----BEGIN SSH HOST KEY FINGERPRINTS-----
   ec2: 256 SHA256:l4UB/neBad9tvkgJf1QZWxheQmR59WgrgzEimCG6kZY no comment (ECDSA)
   ec2: 256 SHA256:kpEa+rw/Uq3zxaYZN8KT501iBtJOIdHG52dFi66EEfQ no comment (ED25519)
   ec2: 2048 SHA256:L8l6pepcA7iqW/jBecQjVZClUrKY+o2cHLI0iHerbVc no comment (RSA)
   ec2: -----END SSH HOST KEY FINGERPRINTS-----
   ```

```
ec2: ###############################################################
```

> **Note**
>
> Hará referencia a esta huella dactilar cuando se conecte a la instancia.

Conéctese a la instancia de Linux desde Linux o macOS mediante SSH.

Puede usar Secure Shell (SSH) para conectarse a su instancia de Linux desde una máquina local, que ejecute un sistema operativo Linux o macOS, o puede utilizar una herramienta de conexión independiente de la plataforma, como EC2 Instance Connect o Session Manager de AWS Systems Manager. Para obtener más información sobre las herramientas independientes de la plataforma, consulte Conexión con la instancia de Linux.

En esta página se explica cómo conectarse a la instancia con un cliente SSH. Para conectarse a la instancia de Linux desde Windows, consulte Conectarse desde Windows.

> **Note**
>
> Si recibe un error al intentar conectarse a su instancia, asegúrese de que la instancia cumple con todos los Requisitos previos para la conexión SSH. Si cumple con todos los requisitos previos y sigue sin poder conectarse a su instancia de Linux, consulte Solución de problemas de conexión a la instancia de Linux.

Contenido

Requisitos previos para la conexión SSH

Antes de conectarse a la instancia de Linux, se deben completar los siguientes requisitos previos.

Comprobar el estado de la instancia

Una vez iniciada la instancia, pueden transcurrir unos minutos hasta que esté lista para conectarse. Verifique que su instancia ha pasado las comprobaciones de estado. Puede ver esta información en la columna Comprobación de estado de la página instancias.

Obtener el nombre DNS público y el nombre de usuario para conectarse a la instancia

Para encontrar el nombre de DNS público o la dirección IP de la instancia y el nombre de usuario que debería utilizar para conectarse a la instancia, consulte Obtenga información sobre su instancia.

Buscar la clave privada y establecer los permisos

Para localizar la clave privada necesaria para conectarse a la instancia y establecer los permisos de clave, consulte Busque la clave privada y establezca permisos..

Instale un cliente SSH en el equipo local según sea necesario

Es posible que el equipo local tenga instalado un cliente SSH de forma predeterminada. Puede verificarlo escribiendo ssh en la línea de comandos. Si su equipo no reconoce el comando, puede instalar un cliente SSH.

- OpenSSH se incluye como componente instalable en las versiones recientes de Windows Server 2019 y Windows 10. Para obtener más información, consulte OpenSSH en Windows.
- Versiones anteriores de Windows: descargar e instalar OpenSSH. Para obtener más información, consulte Win32-OpenSSH.
- Linux y macOS X: descargar e instalar OpenSSH. Para obtener más información, consulte https://www.openssh.com.

Conexión a la instancia de Linux mediante un cliente SSH

Para conectarse a la instancia de Linux mediante un cliente SSH, use el siguiente procedimiento. Si aparece un error al intentar conectarse a la instancia, consulte Solución de problemas de conexión a la instancia de Linux.

Conéctese a la instancia mediante SSH.

1. En una ventana de terminal, utilice el comando ssh para conectarse a la instancia. Especifique la ruta de acceso y el nombre de archivo de la clave privada (`.pem`), el nombre de usuario de la instancia y el nombre de DNS público o la dirección IPv6 de la instancia. Para obtener más

información acerca de cómo encontrar la clave privada, el nombre de usuario de una instancia y el nombre DNS o la dirección IPv6 de una instancia, consulte Busque la clave privada y establezca permisos. y Obtenga información sobre su instancia. Para conectarse a la instancia, utilice uno de los siguientes comandos.

- (DNS público) Para conectarse utilizando el nombre de DNS público de la instancia, escriba el siguiente comando.

```
ssh -i /path/key-pair-name.pem instance-user-name@instance-public-dns-name
```

- (IPv6) Si la instancia tiene una dirección IPv6, también puede utilizar el siguiente comando para conectarse utilizando esta dirección IPv6.

```
ssh -i /path/key-pair-name.pem instance-user-name@instance-IPv6-address
```

Debería ver una respuesta como lo siguiente:

```
The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (198-51-100-1)'
 can't be established.
ECDSA key fingerprint is l4UB/neBad9tvkgJf1QZWxheQmR59WgrgzEimCG6kZY.
Are you sure you want to continue connecting (yes/no)?
```

2. (Opcional) Verifique que la huella digital en la alerta de seguridad coincide con la huella digital que obtuvo anteriormente en (Opcional) Obtenga la huella digital de la instancia. Si estas huellas digitales no coinciden, alguien podría intentar un ataque de intermediarios o man-in-the-middle. Si coinciden, continúe con el siguiente paso.
3. Escriba **yes**.

   Debería ver una respuesta como lo siguiente:

```
Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (ECDSA) to
 the list of known hosts.
```

Transferir archivos a instancias de Linux mediante un cliente SCP

Una de las formas de transferir archivos entre el equipo local y una instancia de Linux consiste en utilizar el protocolo de copia segura (SCP). En esta sección se describe cómo transferir archivos con SCP. El procedimiento es similar al que se debe seguir para conectarse a una instancia con SSH.

Requisitos previos

- Verifique los requisitos previos generales para transferir archivos a la instancia.

  Antes de transferir archivos entre la máquina local y la instancia, realice las siguientes acciones para asegurarse de que dispone de toda la información que necesita.

  - Obtenga información sobre su instancia
  - Busque la clave privada y establezca permisos.
  - (Opcional) Obtenga la huella digital de la instancia
- Instale un cliente SCP

  La mayoría de equipos Linux, Unix y Apple incluyen un cliente SCP de forma predeterminada. Si el equipo no lo incluye, el proyecto OpenSSH proporciona una implementación gratuita de toda la suite de herramientas de SSH, incluido un cliente SCP. Para obtener más información, consulte https://www.openssh.com.

El procedimiento siguiente le guiará a través del uso de SCP para transferir un archivo utilizando el nombre DNS público de la instancia, o la dirección IPv6 si la instancia tiene una.

Para utilizar SCP para transferir archivos entre el equipo y la instancia

1. Determine la ubicación del archivo de origen en el equipo y la ruta de destino en la instancia. En los ejemplos siguientes, el nombre del archivo de clave privada es `key-pair-name.pem`, el archivo que se va a transferir es `my-file.txt`, el nombre de usuario de la instancia es ec2-user, el nombre DNS público de la instancia es `instance-public-dns-name`y la dirección IPv6 de la instancia es `instance-IPv6-address`.
   - (DNS público) Para transferir un archivo al destino de la instancia, escriba el siguiente comando desde el equipo.

     ```
     scp -i /path/key-pair-name.pem /path/my-file.txt ec2-user@instance-public-dns-name:path/
     ```
   - (IPv6) Para transferir un archivo al destino de la instancia si la instancia tiene una dirección IPv6, escriba el siguiente comando desde el equipo. La dirección IPv6 se debe escribir entre corchetes (`[ ]`), a los que se deben aplicar escape (\).

```
scp -i /path/key-pair-name.pem /path/my-file.txt ec2-user@\[instance-IPv6-address\]:path/
```

2. Si aún no se ha conectado a la instancia mediante SSH, verá una respuesta como la siguiente:

```
The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (10.254.142.33)'
can't be established.
RSA key fingerprint is 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f.
Are you sure you want to continue connecting (yes/no)?
```

(Opcional) Si lo desea, puede comprobar que la huella digital de la alerta de seguridad coincide con la huella digital de la instancia. Para obtener más información, consulte (Opcional) Obtenga la huella digital de la instancia.

Escriba **yes**.

3. Si la transferencia se realiza correctamente, la respuesta será similar a la siguiente:

```
Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (RSA)
to the list of known hosts.
my-file.txt                                   100%   480     24.4KB/s   00:00
```

4. Para transferir un archivo en la otra dirección (desde la instancia Amazon EC2 al equipo), revierta el orden de los parámetros de host. Por ejemplo, puede transferir `my-file.txt` desde la instancia de EC2 al destino en el equipo local `my-file2.txt`, como se muestra en los siguientes ejemplos.

   - (DNS público) Para transferir un archivo a un destino del equipo, escriba el siguiente comando desde el equipo.

     ```
     scp -i /path/key-pair-name.pem ec2-user@instance-public-dns-name:path/my-file.txt path/my-file2.txt
     ```

   - (IPv6) Para transferir un archivo a un destino del equipo si la instancia tiene una dirección IPv6, escriba el siguiente comando desde el equipo. La dirección IPv6 se debe escribir entre corchetes ([ ]), a los que se deben aplicar escape (\).

     ```
     scp -i /path/key-pair-name.pem ec2-user@\[instance-IPv6-address\]:path/my-file.txt path/my-file2.txt
     ```

Conéctese a la instancia de Linux desde Windows

Puede utilizar los siguientes métodos para conectarse a la instancia de Linux desde un equipo local que tenga un sistema operativo Windows.

Conéctese a la instancia de Linux desde Windows mediante OpenSSH

En los siguientes procedimientos se muestra cómo puede conectarse a la instancia de Linux desde Windows mediante OpenSSH, una herramienta de conectividad de código abierto para iniciar sesión de forma remota con el protocolo SSH. OpenSSH es compatible con Windows Server 2019 y los sistemas operativos posteriores.

Contenido

Requisitos previos

Antes de conectarse a la instancia de Linux desde Windows mediante OpenSSH, se deben completar los siguientes requisitos previos.

Verifique que la instancia está lista

Una vez iniciada la instancia, pueden transcurrir unos minutos hasta que esté lista para conectarse. Verifique que su instancia ha pasado las comprobaciones de estado. Puede ver esta información en la columna Status check (Comprobación de estado) de la página Instances (instancia[s]).

Verifique los requisitos previos generales para conectarse a la instancia

Para encontrar el nombre de DNS público o la dirección IP de la instancia y el nombre de usuario que debería utilizar para conectarse a la instancia, consulte Obtenga información sobre su instancia.

Verificación de la versión de Windows

Para conectarse a la instancia de Linux desde Windows mediante OpenSSH, la versión de Windows debe ser Windows Server 2019 o posterior.

Verificación de los requisitos previos de PowerShell

Para instalar OpenSSH en el sistema operativo Windows mediante PowerShell, debe ejecutar la versión 5.1 o una posterior de PowerShell, y su cuenta debe pertenecer al grupo de administradores integrado. Ejecute `$PSVersionTable.PSVersion` desde PowerShell para comprobar la versión de PowerShell.

Para comprobar si pertenece al grupo de administradores integrado, ejecute el siguiente comando de PowerShell:

```
(New-Object
 Security.Principal.WindowsPrincipal([Security.Principal.WindowsIdentity]::GetCurrent())).Is
```

Si pertenece al grupo de administradores integrado, la salida es `True`.

Instalación de OpenSSH para Windows mediante PowerShell

A fin de instalar OpenSSH para Windows mediante PowerShell, ejecute el siguiente comando de PowerShell:

```
Add-WindowsCapability -Online -Name OpenSSH.Client~~~~0.0.1.0
```

Resultado previsto:

```
Path          :
Online        : True
RestartNeeded : False
```

Conectarse a la instancia de Linux desde Windows mediante OpenSSH

Tras instalar OpenSSH, utilice el siguiente procedimiento para conectarse a la instancia de Linux desde Windows mediante OpenSSH. Si aparece un error al intentar conectarse a la instancia, consulte Solución de problemas de conexión a la instancia de Linux.

Conectarse a la instancia mediante SSH

1. En PowerShell o en el símbolo del sistema, utilice el comando ssh para conectarse a la instancia. Especifique la ruta de acceso y el nombre de archivo de la clave privada (`.pem`), el nombre de usuario de la instancia y el nombre de DNS público o la dirección IPv6 de la

instancia. Para obtener más información acerca de cómo encontrar la clave privada, el nombre de usuario de una instancia y el nombre DNS o la dirección IPv6 de una instancia, consulte Busque la clave privada y establezca permisos. y Obtenga información sobre su instancia. Para conectarse a la instancia, utilice uno de los siguientes comandos.

- (DNS público) Para conectarse utilizando el nombre de DNS público de la instancia, escriba el siguiente comando.

```
ssh -i /path/key-pair-name.pem instance-user-name@instance-public-dns-name
```

- (IPv6) Si la instancia tiene una dirección IPv6, también puede utilizar el siguiente comando para conectarse utilizando esta dirección IPv6.

```
ssh -i /path/key-pair-name.pem instance-user-name@instance-IPv6-address
```

Debería ver una respuesta como lo siguiente:

```
The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (198-51-100-1)'
 can't be established.
ECDSA key fingerprint is l4UB/neBad9tvkgJf1QZWxheQmR59WgrgzEimCG6kZY.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

2. (Opcional) Verifique que la huella digital en la alerta de seguridad coincide con la huella digital que obtuvo anteriormente en (Opcional) Obtenga la huella digital de la instancia. Si estas huellas digitales no coinciden, alguien podría intentar un ataque de intermediarios o man-in-the-middle. Si coinciden, continúe con el siguiente paso.
3. Escriba **yes**.

   Debería ver una respuesta como lo siguiente:

```
Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (ECDSA) to
 the list of known hosts.
```

Desinstalación de OpenSSH de Windows mediante PowerShell

A fin de desinstalar OpenSSH de Windows mediante PowerShell, ejecute el siguiente comando de PowerShell:

```
Remove-WindowsCapability -Online -Name OpenSSH.Client~~~~0.0.1.0
```

Resultado previsto:

```
Path          :
Online        : True
RestartNeeded : True
```

Conéctese a la instancia de Linux desde Windows con PuTTY

Si ejecuta Windows Server 2019 o posterior, le recomendamos usar OpenSSH, que es una herramienta de conectividad de código abierto para iniciar sesión de forma remota con el protocolo SSH. Para obtener información sobre los pasos para conectarse a una instancia de Linux desde Windows mediante OpenSSH, consulte Conéctese a la instancia de Linux desde Windows mediante OpenSSH.

Las siguientes instrucciones explican cómo conectarse a la instancia mediante PuTTY, un cliente SSH para Windows. Si aparece un error al intentar conectarse a la instancia, consulte Solución de problemas de conexión a la instancia de Linux.

Contenido

Requisitos previos

Antes de conectarse a la instancia de Linux mediante PuTTY, se deben completar los siguientes requisitos previos:

Verifique que la instancia está lista

> Una vez iniciada la instancia, pueden transcurrir unos minutos hasta que esté lista para conectarse. Verifique que su instancia ha pasado las comprobaciones de estado. Puede ver esta información en la columna Status check (Comprobación de estado) de la página Instances (instancia[s]).

Verifique los requisitos previos generales para conectarse a la instancia

Para encontrar el nombre de DNS público o la dirección IP de la instancia y el nombre de usuario que debería utilizar para conectarse a la instancia, consulte Obtenga información sobre su instancia.

Instale PuTTY en su equipo local

Descargue e instale PuTTY desde la página de descarga de PuTTY. Si ya tiene instalada una versión antigua de PuTTY, le recomendamos que descargue la última versión. Asegúrese de instalar el conjunto completo.

Convierta su clave .pem privada en .ppk con PuTTYgen

Para el par de claves especificado al iniciar la instancia, si eligió crear la clave privada en formato .pem, debe convertirla en un archivo .ppk para usarla con PuTTY. Busque el archivo .pem privado y, a continuación, siga los pasos que se indican en la siguiente sección.

Convierta su clave privada utilizando PuTTYgen

PuTTY no admite de forma nativa el formato PEM para claves SSH. PuTTY proporciona una herramienta llamada PuTTYgen, la cual convierte claves al formato requerido PPK para PuTTY. Debe convertir su clave privada (archivo .pem) a este formato (archivo .ppk) como se indica a continuación para conectarse a la instancia mediante PuTTY.

Para convertir una clave .pem privada al formato .ppk

1. En el menú Start (Inicio), elija All Programs (Todos los programas), PuTTY, PuTTYgen.
2. En Type of key to generate (Tipo de clave a generar), elija RSA. Si la versión de PuTTYGen no incluye esta opción, elija SSH-2 RSA.

3. Elija Load (Cargar). De forma predeterminada, PuTTYgen muestra solo archivos con la extensión `.ppk`. Para localizar el archivo `.pem`, seleccione la opción de mostrar todos los tipos de archivo.

4. Seleccione el archivo `.pem` para el par de claves que especificó cuando lanzó la instancia y, a continuación, elija Open (Abrir). PuTTYgen muestra un aviso de que el archivo `.pem` se ha importado correctamente. Seleccione OK.
5. Elija Save private key (Guardar la clave privada) para guardar la clave en formato que PuTTY pueda utilizar. PuTTYgen mostrará una advertencia acerca de guardar la clave sin una frase de contraseña. Elija Yes (Sí).

> **Note**
>
> Una contraseña de una clave privada es una capa adicional de protección. Incluso si se descubriera su clave privada, no se puede usar sin la contraseña. El inconveniente de usar una contraseña es que dificulta la automatización puesto que la intervención humana es necesaria para iniciar una sesión en una instancia o para copiar archivos en una instancia.

6. Especifique el mismo nombre para la clave que utilizó para el par de claves (por ejemplo `key-pair-name`) y elija Save (Guardar). PuTTY añade la extensión de archivo `.ppk` automáticamente.

La clave privada está ahora en el formato correcto para su uso con PuTTY. Ya puede conectarse a la instancia mediante el cliente SSH de PuTTY.

Conexión con la instancia de Linux

Para conectarse a la instancia de Linux mediante PuTTY, use el siguiente procedimiento. Necesita el archivo `.ppk` que creó para la clave privada. Para obtener más información, consulte Convierta su clave privada utilizando PuTTYgen en la sección anterior. Si aparece un error al intentar conectarse a la instancia, consulte Solución de problemas de conexión a la instancia de Linux.

Última versión probada de PuTTY: .78

Para conectarse a la instancia mediante PuTTY

1. Inicie PuTTY (en el menú Inicio, busque PuTTY y, a continuación, elija Abrir).
2. En el panel Category (Categoría), elija Session (Sesión) y rellene los siguientes campos:

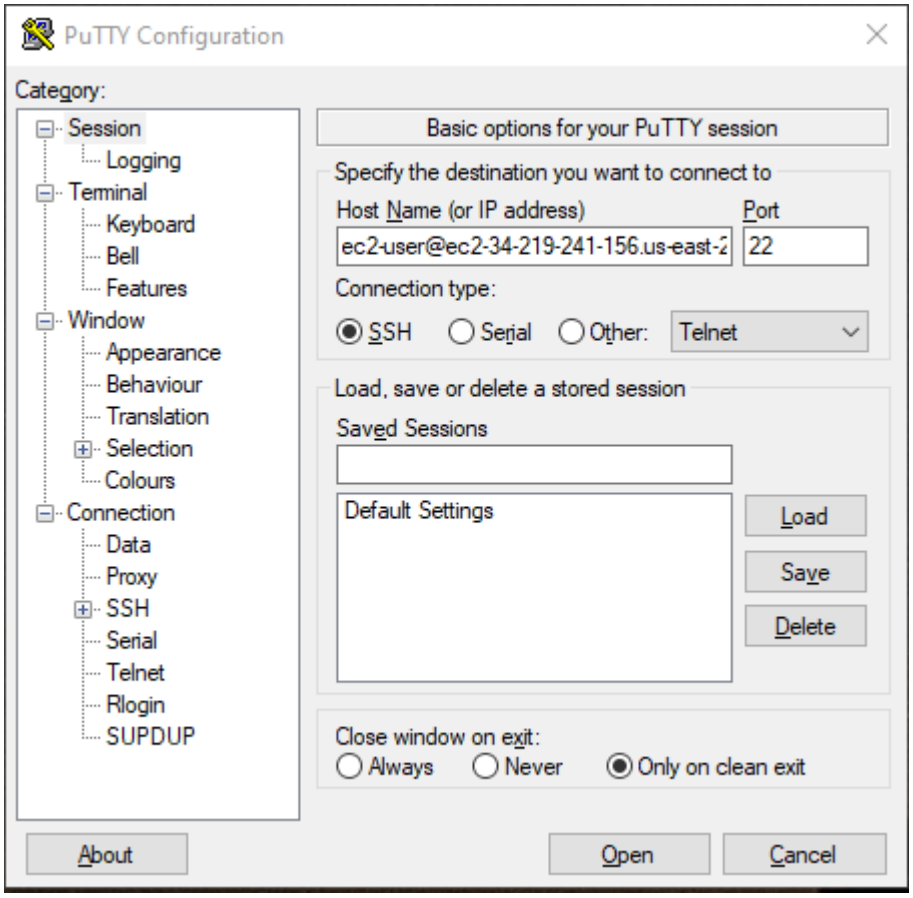
a. En el cuadro Host Name (Nombre de host) siga uno de estos procedimientos:

   - (DNS público) Para conectarse utilizando el nombre DNS público de la instancia, escriba *instance-user-name*@*instance-public-dns-name*.
   - (IPv6) Como opción, si la instancia tiene una dirección IPv6, para conectarse utilizando esta dirección IPv6, escriba *instance-user-name*@*instance-IPv6-address*.

   Para obtener información acerca de cómo obtener el nombre de usuario de la instancia y el nombre de DNS público o la dirección IPv6 de la instancia, consulte Obtenga información sobre su instancia.

b. Asegúrese de que el valor del Port (Puerto) es 22.

c. En Connection type (Tipo de conexión), seleccione SSH.



3. (Opcional) Puede configurar PuTTY para que envíe datos “keepalive” a intervalos regulares para mantener la sesión activa. Esto es útil para evitar desconectarse de su instancia por inactividad en la sesión. En el panel Categoría, elija Conexión y, a continuación, ingrese el intervalo

deseado en el campo Segundos entre keepalives. Por ejemplo, si su sesión se desconecta tras 10 minutos de inactividad, escriba 180 para que PuTTY envíe datos “keepalive” cada 3 minutos.

4. En el panel Categoría, expanda Conexión, SSH y Autenticación. Elija Credenciales.
5. Junto a Archivo de clave privada para la autenticación, seleccione Examinar. En el cuadro de diálogo Seleccionar archivo de clave privada, seleccione el archivo `.ppk` que generó para su par de claves. Puede hacer doble clic en el archivo o seleccionar Abrir en el cuadro de diálogo Seleccionar archivo de clave privada.
6. (Opcional) Si tiene previsto volver a conectar esta sesión después de esta sesión, puede guardar la sesión informativa para usarla en el futuro. En el panel Categoría, seleccione Sesión. Ingrese un nombre para la sesión en Sesiones guardadas y, a continuación, elija Guardar.
7. Para conectarse a la instancia, seleccione Abrir.
8. Si esta es la primera vez que se conecta a esta instancia, PuTTY muestra un cuadro de diálogo de alerta de seguridad que le pregunta si tiene confianza en el host al que se está conectando.

    a. (Opcional) Verifique que la huella digital en el cuadro de diálogo de la alerta de seguridad coincide con la huella digital que obtuvo anteriormente en (Opcional) Obtenga la huella digital de la instancia. Si estas huellas digitales no coinciden, alguien podría intentar un ataque man-in-the-middle (MITM). Si coinciden, continúe con el siguiente paso.

    b. Elija Aceptar. Se abre una ventana y está conectado a la instancia.

> **Note**
>
> Si especificó una frase de contraseña al convertir la clave privada al formato PuTTY, deberá indicar la contraseña cuando inicie sesión en la instancia.

Si aparece un error al intentar conectarse a la instancia, consulte Solución de problemas de conexión a la instancia de Linux.

Transferir archivos a la instancia de Linux mediante el cliente Secure Copy de PuTTY

El cliente Secure Copy de PuTTY (PSCP) es una herramienta de línea de comandos que puede usar para transferir archivos entre el equipo Windows y la instancia de Linux. Si prefiere una interfaz de usuario gráfica (GUI), puede usar una herramienta de GUI de código abierto llamada WinSCP. Para obtener más información, consulte Transferir archivos de la instancia de Linux mediante WinSCP.

Para usar PSCP, necesita la clave privada que generó en Convierta su clave privada utilizando PuTTYgen. También necesita el nombre de DNS público de su instancia de Linux o la dirección IPv6 si su instancia tiene una.

El siguiente ejemplo transfiere el archivo `Sample_file.txt` desde la unidad C:\ de un equipo Windows al directorio principal `instance-user-name` de una instancia de Amazon Linux: Para transferir un archivo, utilice uno de los siguientes comandos.

- (DNS público) Para transferir un archivo utilizando el nombre DNS público de la instancia, escriba el siguiente comando.

```
pscp -i C:\path\my-key-pair.ppk C:\path\Sample_file.txt instance-user-name@instance-public-dns-name:/home/instance-user-name/Sample_file.txt
```

- (IPv6) Como opción, si la instancia tiene una dirección IPv6, para transferir un archivo utilizando la dirección IPv6 de su instancia, escriba el siguiente comando. La dirección IPv6 se debe escribir entre corchetes (`[ ]`).

```
pscp -i C:\path\my-key-pair.ppk C:\path\Sample_file.txt instance-user-name@[instance-IPv6-address]:/home/instance-user-name/Sample_file.txt
```

Transferir archivos de la instancia de Linux mediante WinSCP

WinSCP es un administrador de archivos basado en GUI para Windows que le permite cargar y transferir archivos a un equipo remoto mediante los protocolos SFTP, SCP, FTP y FTPS. WinSCP le permite arrastrar y soltar archivos desde el equipo con Windows a la instancia de Linux, o sincronizar estructuras de directorios completas entre los dos sistemas.

Requisitos

- Debe tener la clave privada que se generó en Convierta su clave privada utilizando PuTTYgen.
- También necesita el nombre DNS público de la instancia de Linux.
- La instancia de Linux debe tener instalado `scp`. En algunos sistemas operativos, puede instalar el paquete `openssh-clients`. En otros, como la AMI optimizada para Amazon ECS, puede instalar el paquete `scp`. Compruebe la documentación de su distribución Linux.

Para conectarse a la instancia mediante WinSCP

1. Descargue e instale WinSCP desde http://winscp.net/eng/download.php. La mayoría de usuarios no necesitará modificar las opciones de instalación predeterminadas.
2. Inicie WinSCP.
3. En la pantalla inicio de sesión de WinSCP en Nombre de host, escriba una de las siguientes opciones:
   - (DNS público o dirección IPv4) Para iniciar sesión con el nombre de DNS público o la dirección IPv4 pública de la instancia, introduzca el nombre de DNS público o la dirección IPv4 pública de la instancia.
   - (IPv6) Como opción, si la instancia tiene una dirección IPv6, para iniciar sesión utilizando la dirección IPv6 de la instancia, escriba la dirección IPv6 de la instancia.
4. En Nombre de usuario, escriba el nombre de usuario predeterminado para la AMI.
   - Para AL2023, Amazon Linux 2 o la AMI de Amazon Linux, el nombre de usuario es `ec2-user`.
   - Para una AMI de CentOS, el nombre de usuario es `centos` o `ec2-user`.
   - Para una AMI de Debian, el nombre de usuario es `admin`.
   - Para una AMI de Fedora, el nombre de usuario es `fedora` o `ec2-user`.
   - Para una AMI de RHEL, el nombre de usuario es `ec2-user` o `root`.
   - Para una AMI de SUSE, el nombre de usuario es `ec2-user` o `root`.
   - Para una AMI de Ubuntu, el nombre de usuario es `ubuntu`.
   - Para una AMI de Oracle, el nombre de usuario es `ec2-user`.
   - Para una AMI de Bitnami, el nombre de usuario es `bitnami`.

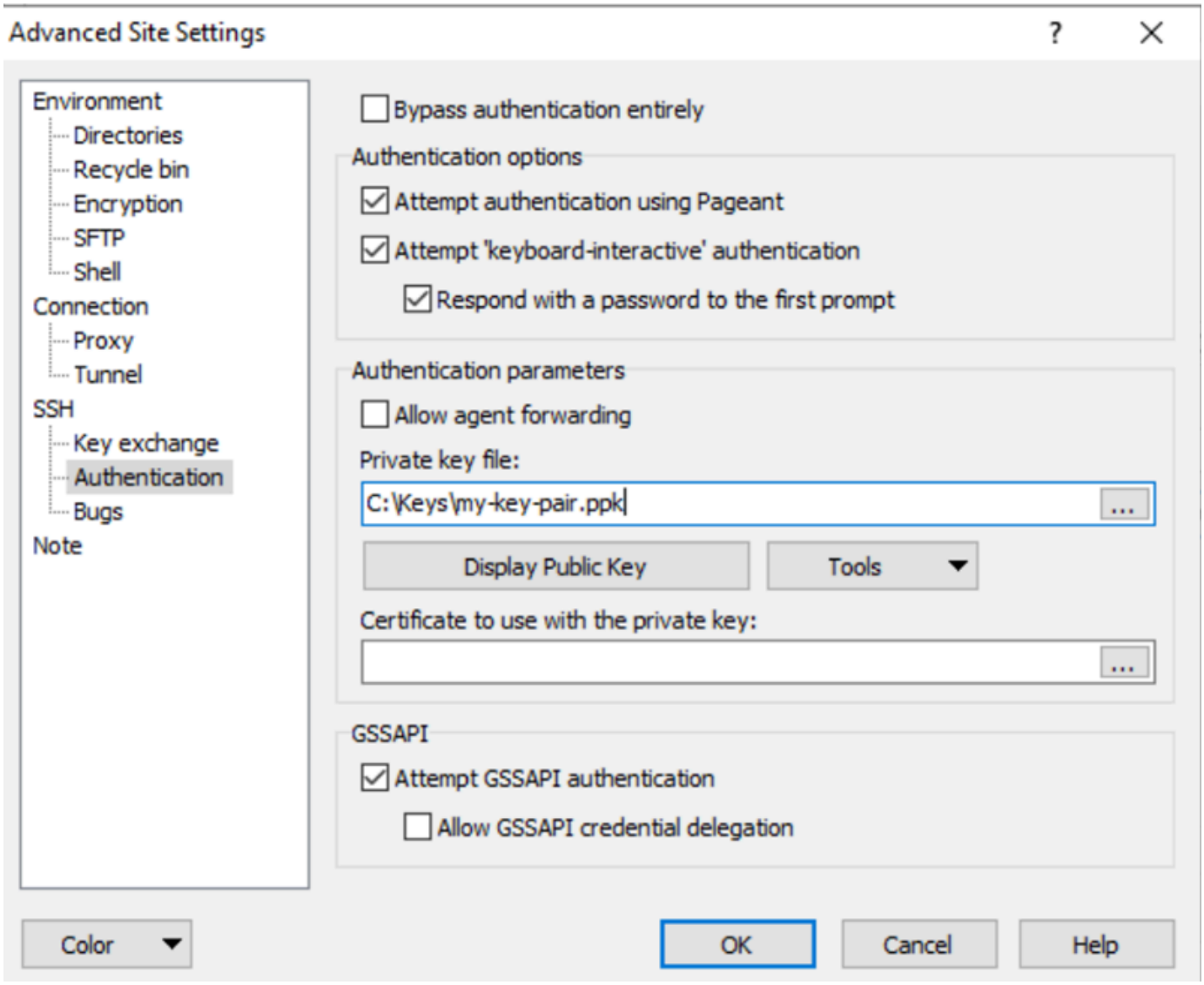
   > **Note**
   >
   > Para encontrar el nombre de usuario predeterminado para otras distribuciones de Linux, consulte con el proveedor de AMI.

5. Especifique la clave privada de la instancia.
   a. Elija la opción Avanzado... botón.
   b. En SSH, selecciona Autenticación.

c. Especifique la ruta del archivo de clave privada o elija la... botón para buscar el archivo del key pair.

d. Seleccione Aceptar.

Aquí hay una captura de pantalla de WinSCP versión 6.1:

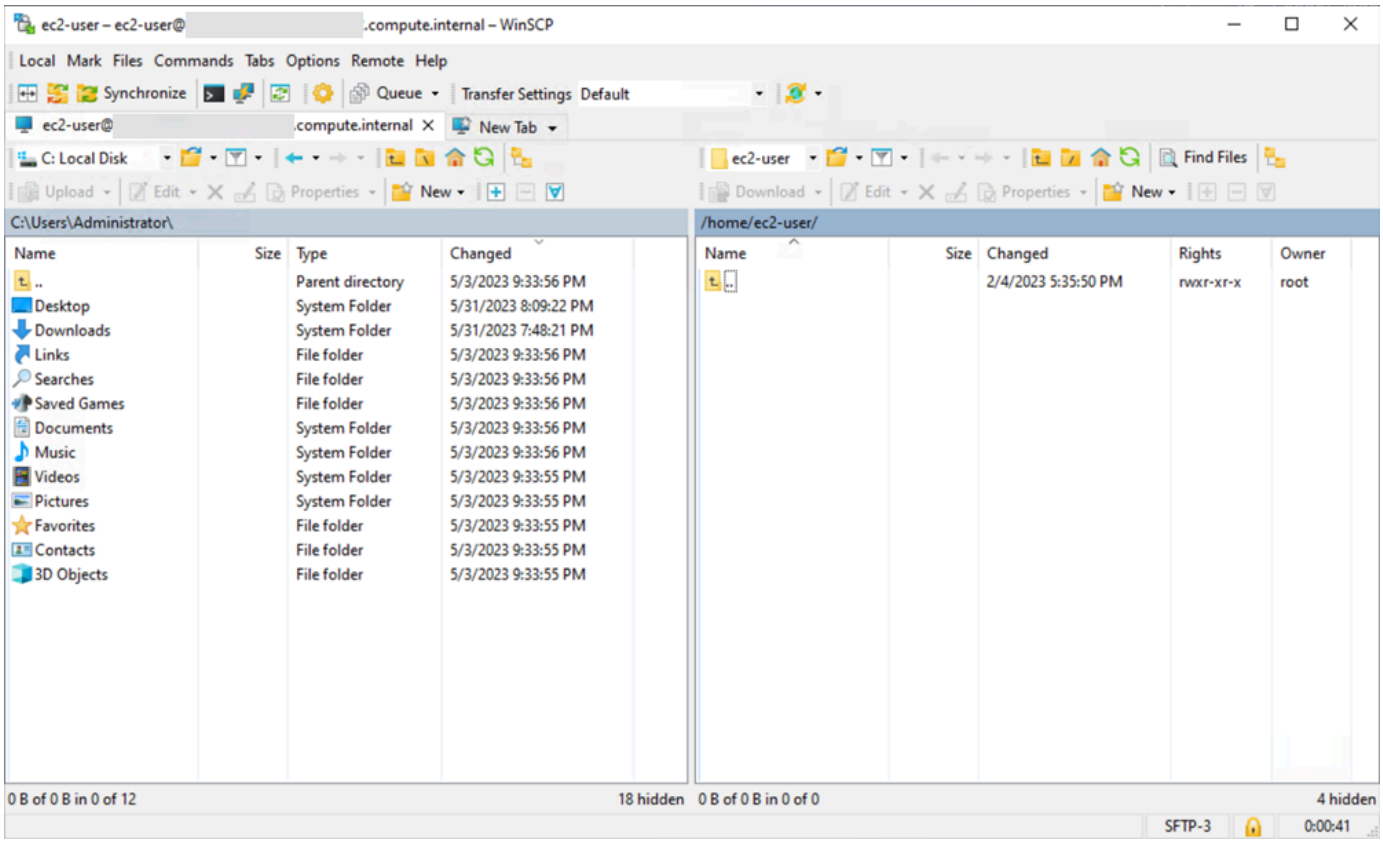


WinSCP requiere un archivo () de clave privada de Pu (`.ppk`). Puede convertir un archivo de clave de seguridad `.pem` en el formato `.ppk` mediante PuTTYgen. Para obtener más información, consulte Convierta su clave privada utilizando PuTTYgen.

6. De forma opcional, en el panel izquierdo, elija Directories (Directorios). En Remote directory (Directorio remoto), introduzca la ruta del directorio al que se añaden los archivos. Para abrir la configuración avanzada, para las versiones más recientes de WinSCP, elija Advanced

(Avanzada). Para encontrar la configuración del Remote directory (Directorio remoto), en Environment (Entorno), elija Directories (Directorios).

7. Seleccione Login (Iniciar sesión). Para añadir la huella digital del host a la caché del host, elija Yes (Sí).



8. Una vez establecida la conexión, la instancia de Linux aparece a la derecha y el equipo local a la izquierda en la ventana de conexión. Puede arrastrar y soltar archivos entre el sistema de archivos remoto y la máquina local. Para obtener más información sobre WinSCP, consulte la documentación del proyecto en http://winscp.net/eng/docs/start.

   Si recibe un error que indica que no puede ejecutar SCP para iniciar la transferencia, compruebe que scp esté instalado en la instancia de Linux.

Conéctese a instancias de Linux desde Windows con Windows Subsystem for Linux (WSL)

Después de iniciar la instancia, puede conectarse a ella y usarla como si fuera un equipo.

Las siguientes instrucciones explican cómo conectarse a la instancia con una distribución de Linux en el Windows Subsystem for Linux (WSL). WSL se descarga gratuitamente y le permite ejecutar

herramientas de línea de comandos de Linux nativas directamente en Windows, junto con su escritorio de Windows tradicional, sin el recargo de una máquina virtual.

Al instalar WSL, puede utilizar un entorno Linux nativo para conectar a sus instancias de EC2 Linux en lugar de utilizar PuTTY o PuTTYgen. El entorno de Linux facilita la conexión a las instancias Linux ya que dispone de un cliente SSH nativo que puede utilizar para conectar a sus instancias Linux y cambiar los permisos del archivo de claves .pem. La consola de Amazon EC2 proporciona el comando SSH para conectar a la instancia Linux y puede obtener resultados detallados desde el comando SSH para solución de problemas. Para obtener más información, consulte la documentación de Windows Subsystem for Linux.

> **Note**
>
> Después de haber instalado WSL, todos los requisitos y pasos son los mismos que se describen en Conéctese a la instancia de Linux desde Linux o macOS mediante SSH. y la experiencia es como utilizar el Linux nativo.

Si aparece un error al intentar conectarse a la instancia, consulte Solución de problemas de conexión a la instancia de Linux.

Contenido

Requisitos previos

Antes de conectarse a la instancia de Linux, debe completar los siguientes requisitos previos.

Verifique que la instancia está lista

Una vez iniciada la instancia, pueden transcurrir unos minutos hasta que esté lista para conectarse. Verifique que su instancia ha pasado las comprobaciones de estado. Puede ver esta información en la columna Status check (Comprobación de estado) de la página Instances (instancia[s]).

Verifique los requisitos previos generales para conectarse a la instancia

Para encontrar el nombre de DNS público o la dirección IP de la instancia y el nombre de usuario que debería utilizar para conectarse a la instancia, consulte Obtenga información sobre su instancia.

Instalar el Windows Subsystem for Linux (WSL) y una distribución de Linux en su equipo local

Instale el WSL y una distribución de Linux utilizando las instrucciones de la Guía de instalación de Windows 10. El ejemplo que aparece en las instrucciones instala la distribución Ubuntu de Linux, pero puede instalar cualquier distribución. Se le solicita que reinicie su equipo para que se apliquen los cambios.

Copiar la clave privada de Windows a WSL

En una ventana de terminal de WSL, copie el archivo `.pem` (para el par de claves que especificó cuando lanzó la instancia) de Windows a WSL. Anote la ruta completa al archivo `.pem` en WSL que utilizar al conectar a la instancia. Para obtener información acerca de cómo especificar la ruta a su disco duro de Windows, consulte How do I access my C drive? Para obtener más información acerca de los pares de claves y las instancias de Windows, consulte Pares de claves de Amazon EC2 e instancias de Windows.

```
cp /mnt/<Windows drive letter>/path/my-key-pair.pem ~/WSL-path/my-key-pair.pem
```

Conexión a la instancia de Linux con WSL

Siga este procedimiento para conectar a la instancia Linux utilizando el Windows Subsystem for Linux (WSL). Si aparece un error al intentar conectarse a la instancia, consulte Solución de problemas de conexión a la instancia de Linux.

Para conectarse a la instancia mediante SSH

1. En una ventana de terminal, utilice el comando ssh para conectarse a la instancia. Especifique la ruta de acceso y el nombre de archivo de la clave privada (`.pem`), el nombre de usuario de la instancia y el nombre de DNS público o la dirección IPv6 de la instancia. Para obtener más información acerca de cómo encontrar la clave privada, el nombre de usuario de una instancia y el nombre DNS o la dirección IPv6 de una instancia, consulte Busque la clave privada y establezca permisos. y Obtenga información sobre su instancia. Para conectarse a la instancia, utilice uno de los siguientes comandos.

- (DNS público) Para conectarse utilizando el nombre de DNS público de la instancia, escriba el siguiente comando.

```
ssh -i /path/key-pair-name.pem instance-user-name@my-instance-public-dns-name
```

- (IPv6) Como opción, si la instancia tiene una dirección IPv6, puede conectarse a la instancia mediante su dirección IPv6. Especifique el comando ssh con la ruta al archivo de clave privada (.pem), el nombre de usuario adecuado y la dirección IPv6.

```
ssh -i /path/key-pair-name.pem instance-user-name@my-instance-IPv6-address
```

Debería ver una respuesta como lo siguiente:

```
The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (10.254.142.33)'
can't be established.
RSA key fingerprint is 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f.
Are you sure you want to continue connecting (yes/no)?
```

2. (Opcional) Verifique que la huella digital en la alerta de seguridad coincide con la huella digital que obtuvo anteriormente en (Opcional) Obtenga la huella digital de la instancia. Si estas huellas digitales no coinciden, alguien podría intentar un ataque man-in-the-middle (MITM). Si coinciden, continúe con el siguiente paso.
3. Escriba `yes`.

   Debería ver una respuesta como lo siguiente:

```
Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (RSA)
to the list of known hosts.
```

Transferir archivos a instancias de Linux desde Linux mediante SCP

Una de las formas de transferir archivos entre el equipo local y una instancia de Linux consiste en utilizar el protocolo de copia segura (SCP). En esta sección se describe cómo transferir archivos con SCP. El procedimiento es similar al que se debe seguir para conectarse a una instancia con SSH.

Requisitos previos

- Verifique los requisitos previos generales para transferir archivos a la instancia.

Antes de transferir archivos entre la máquina local y la instancia, realice las siguientes acciones para asegurarse de que dispone de toda la información que necesita.

- Obtenga información sobre su instancia
- Busque la clave privada y establezca permisos.
- (Opcional) Obtenga la huella digital de la instancia

- Instale un cliente SCP

  La mayoría de equipos Linux, Unix y Apple incluyen un cliente SCP de forma predeterminada. Si el equipo no lo incluye, el proyecto OpenSSH proporciona una implementación gratuita de toda la suite de herramientas de SSH, incluido un cliente SCP. Para obtener más información, consulte https://www.openssh.com.

El siguiente procedimiento muestra cómo usar SCP para transferir un archivo. Si ya se ha conectado a la instancia con SSH y ha verificado sus huellas digitales, puede comenzar con el paso que contiene el comando SCP (paso 4).

Para usar SCP para transferir un archivo

1. Transfiera un archivo a su instancia utilizando el nombre DNS público de la instancia. Por ejemplo, si el nombre del archivo de clave privada es `key-pair-name`, el archivo para transferir es `SampleFile.txt`, el nombre de usuario es `instance-user-name` y el nombre de DNS público de la instancia es `my-instance-public-dns-name` o la dirección IPv6 es `my-instance-IPv6-address`, utilice los siguientes comandos para copiar el archivo en el directorio principal `instance-user-name`:
   - (DNS público) Para transferir un archivo utilizando el nombre DNS público de la instancia, escriba el siguiente comando.

     ```
     scp -i /path/key-pair-name.pem /path/SampleFile.txt instance-user-name@my-instance-public-dns-name:~
     ```

   - (IPv6) Como opción, si la instancia tiene una dirección IPv6, puede transferir un archivo utilizando la dirección IPv6 de la instancia. La dirección IPv6 se debe escribir entre corchetes (`[ ]`), a los que se deben aplicar escape (\).

     ```
     scp -i /path/key-pair-name.pem /path/SampleFile.txt instance-user-name@\[my-instance-IPv6-address\]:~
     ```

Debería ver una respuesta como lo siguiente:

```
The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (10.254.142.33)'
can't be established.
RSA key fingerprint is 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f.
Are you sure you want to continue connecting (yes/no)?
```

2. (Opcional) Verifique que la huella digital en la alerta de seguridad coincide con la huella digital que obtuvo anteriormente en (Opcional) Obtenga la huella digital de la instancia. Si estas huellas digitales no coinciden, alguien podría intentar un ataque man-in-the-middle (MITM). Si coinciden, continúe con el siguiente paso.
3. Escriba **`yes`**.

   Debería ver una respuesta como lo siguiente:

   ```
   Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (RSA)
   to the list of known hosts.
   Sending file modes: C0644 20 SampleFile.txt
   Sink: C0644 20 SampleFile.txt
   SampleFile.txt                                100%   20     0.0KB/s   00:00
   ```

   Si recibe un error “bash: scp: command not found”, primero debe instalar scp en la instancia de Linux. Para algunos sistemas operativos, esto está ubicado en el paquete `openssh-clients`. Para las variantes de Amazon Linux, como la AMI optimizada para Amazon ECS, utilice el comando siguiente para instalar scp:

   ```
   [ec2-user ~]$ sudo yum install -y openssh-clients
   ```

4. Para transferir archivos en la otra dirección (desde la instancia Amazon EC2 al equipo local), revierta el orden de los parámetros de host. Por ejemplo, para transferir el archivo `SampleFile.txt` desde la instancia de EC2 de nuevo al directorio principal en el equipo local como `SampleFile2.txt`, use uno de los siguientes comandos en el equipo local.

   - (DNS público) Para transferir un archivo utilizando el nombre DNS público de la instancia, escriba el siguiente comando.

     ```
     scp -i /path/key-pair-name.pem instance-user-
     name@ec2-198-51-100-1.compute-1.amazonaws.com:~/SampleFile.txt ~/
     SampleFile2.txt
     ```

- (IPv6) Como alternativa, si la instancia tiene una dirección IPv6, para transferir archivos en la otra dirección utilizando la dirección IPv6 de la instancia, escriba el siguiente comando.

```
scp -i /path/key-pair-name.pem instance-user-name@
\[2001:db8:1234:1a00:9691:9503:25ad:1761\]:~/SampleFile.txt ~/SampleFile2.txt
```

Desinstalar WSL

Para obtener información sobre la desinstalación de Windows Subsystem for Linux, consulte How do I uninstall a WSL Distribution?

Conéctese a la instancia de Linux con EC2 Instance Connect

Amazon EC2 Instance Connect es una forma simple y segura de conectarse a las instancias de Linux con Secure Shell (SSH). Con EC2 Instance Connect, puede utilizar políticas de AWS Identity and Access Management (IAM) y entidades principales para controlar el acceso SSH a las instancias y eliminar la necesidad de compartir y administrar las claves SSH. Todas las solicitudes de conexión con EC2 Instance Connect se registran en AWS CloudTrail de modo que puede auditar las solicitudes de conexión.

Puede usar EC2 Instance Connect para conectarse a las instancias con la consola de Amazon EC2 o el cliente SSH que prefiera.

Cuando se conecta a una instancia con EC2 Instance Connect, la API de Instance Connect inserta una clave pública SSH en los metadatos de la instancia, donde permanece por 60 segundos. La política de IAM asociada a su usuario le autoriza a insertar la clave pública en los metadatos de la instancia. El daemon SSH utiliza `AuthorizedKeysCommand` y `AuthorizedKeysCommandUser`, que se configuró cuando se instaló Instance Connect, para buscar la clave pública en los metadatos de la instancia para su autenticación y la conecta a la instancia.

Puede utilizar EC2 Instance Connect para conectarse a instancias que tienen direcciones IP públicas o privadas. Para obtener más información, consulte Conexión mediante EC2 Instance Connect.

Para ver una entrada de blog que explique cómo mejorar la seguridad de los hosts bastión con EC2 Instance Connect, consulte Protección de los hosts bastión con Amazon EC2 Instance Connect.

> **Tip**
>
> EC2 Instance Connect es una de las opciones para conectarse a la instancia de Linux. Para otras opciones, consulte Conexión con la instancia de Linux. Para conectarse a una instancia de Windows, consulte Conexión con la instancia de Windows de.

Contenido

Tutorial: Cómo completar la configuración necesaria para conectarse a la instancia mediante EC2 Instance Connect

Para conectarse a la instancia mediante EC2 Instance Connect en la consola de Amazon EC2, debe completar la configuración previa que le permitirá conectarse correctamente a la instancia. El objetivo de este tutorial es guiarlo a través de las tareas necesarias para completar la configuración previa.

Información general del tutorial

En este tutorial, deberá completar las cuatro tareas detalladas a continuación:

- Tarea 1: Crear y asociar una política de IAM que le permita utilizar EC2 Instance Connect

  En primer lugar, debe crear una política de IAM que contenga los permisos de IAM que le permitirán introducir una clave pública en los metadatos de la instancia. Deberá asociar esta política a su identidad de IAM (usuario, grupo de usuarios o rol) para que su identidad de IAM obtenga estos permisos.
- Tarea 2: Crear un grupo de seguridad que permita el tráfico entrante desde el servicio EC2 Instance Connect a la instancia

A continuación, deberá crear un grupo de seguridad que permita el tráfico desde el servicio EC2 Instance Connect a la instancia. Esto es necesario cuando utiliza EC2 Instance Connect en la consola de Amazon EC2 para conectarse a la instancia.

- Tarea 3: Iniciar la instancia

  A continuación, deberá lanzar una instancia de EC2 con una AMI preinstalada en EC2 Instance Connect y agregar el grupo de seguridad que creó en el paso anterior.

- Tarea 4: Conectarse a la instancia

  Por último, deberá utilizar EC2 Instance Connect en la consola de Amazon EC2 para conectarse a la instancia. Si puede conectarse, esto significa que la configuración previa que completó en las tareas 1, 2 y 3 se realizó correctamente.

Tarea 1: Crear y asociar una política de IAM que le permita utilizar EC2 Instance Connect

Cuando se conecta a una instancia con EC2 Instance Connect, la API de EC2 Instance Connect inserta una clave pública SSH en los metadatos de la instancia, donde permanece por 60 segundos. Necesita una política de IAM asociada a su identidad de IAM (usuario, grupo de usuarios o rol) a fin de obtener el permiso necesario para insertar la clave pública en los metadatos de la instancia.

Objetivo de la tarea

En esta tarea, creará la política de IAM mediante la que se concede el permiso para insertar la clave pública en la instancia. La acción específica que debe permitir es `ec2-instance-connect:SendSSHPublicKey`. También debe permitir la acción `ec2:DescribeInstances` para poder ver y seleccionar la instancia en la consola de Amazon EC2.

Una vez creada la política, deberá asociar esta política a su identidad de IAM (usuario, grupo de usuarios o rol) para que esta obtenga los permisos.

Deberá crear una política con la siguiente configuración:

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": "ec2-instance-connect:SendSSHPublicKey",
            "Resource": "*"
        },
```

```
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeInstances",
            "Resource": "*"
        }
    ]
}
```

> **Important**
>
> La política de IAM creada en este tutorial es muy permisiva; le permite conectarse a cualquier instancia mediante cualquier nombre de usuario de AMI. Utilizamos esta política altamente permisiva para que el tutorial sea sencillo y se enfoque en las configuraciones específicas que se enseñan en él. Sin embargo, en un entorno de producción, le recomendamos que la política de IAM esté configurada para proporcionar permisos con privilegios mínimos. Para ver ejemplos de políticas de IAM, consulte Concesión de permisos de IAM para EC2 Instance Connect.

Pasos para crear y adjuntar la política de IAM

Siga estos pasos para crear y asociar la política de IAM. Para ver una animación de los pasos, consulte Ver una animación: crear una política de IAM y Ver animación: Asociar una política de IAM.

Cómo crear y asociar una política de IAM que le permita usar EC2 Instance Connect para conectarse a las instancias

1. Primero: crear la política de IAM
    a. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
    b. En el panel de navegación, seleccione Políticas.
    c. Elija Create Policy (Crear política).
    d. En la página Especificar permiso, haga lo siguiente:
        i. En Servicio, elija EC2 Instance Connect.
        ii. En Acciones permitidas, en el campo de búsqueda, comience a escribir **send** para ver las acciones relevantes y, a continuación, seleccione SendSSHPublicKey.
        iii. En Recursos, elija Todos. Para un entorno de producción, se recomienda especificar la instancia por su ARN, pero, en este tutorial, se permiten todas las instancias.

iv. Elija Add more permissions.

v. En Servicio, elija EC2.

vi. En Acciones permitidas, en el campo de búsqueda, comience a escribir **`describein`** para ver las acciones relevantes y, a continuación, seleccione DescribeInstances.

vii. Elija Siguiente.

e. En la página Revisar y crear, haga lo siguiente:

i. En Nombre de política, escriba un nombre para la política.

ii. Elija Crear política.

2. A continuación, asocie la política a su identidad

a. En la consola de IAM, en el panel de navegación, elija Políticas.

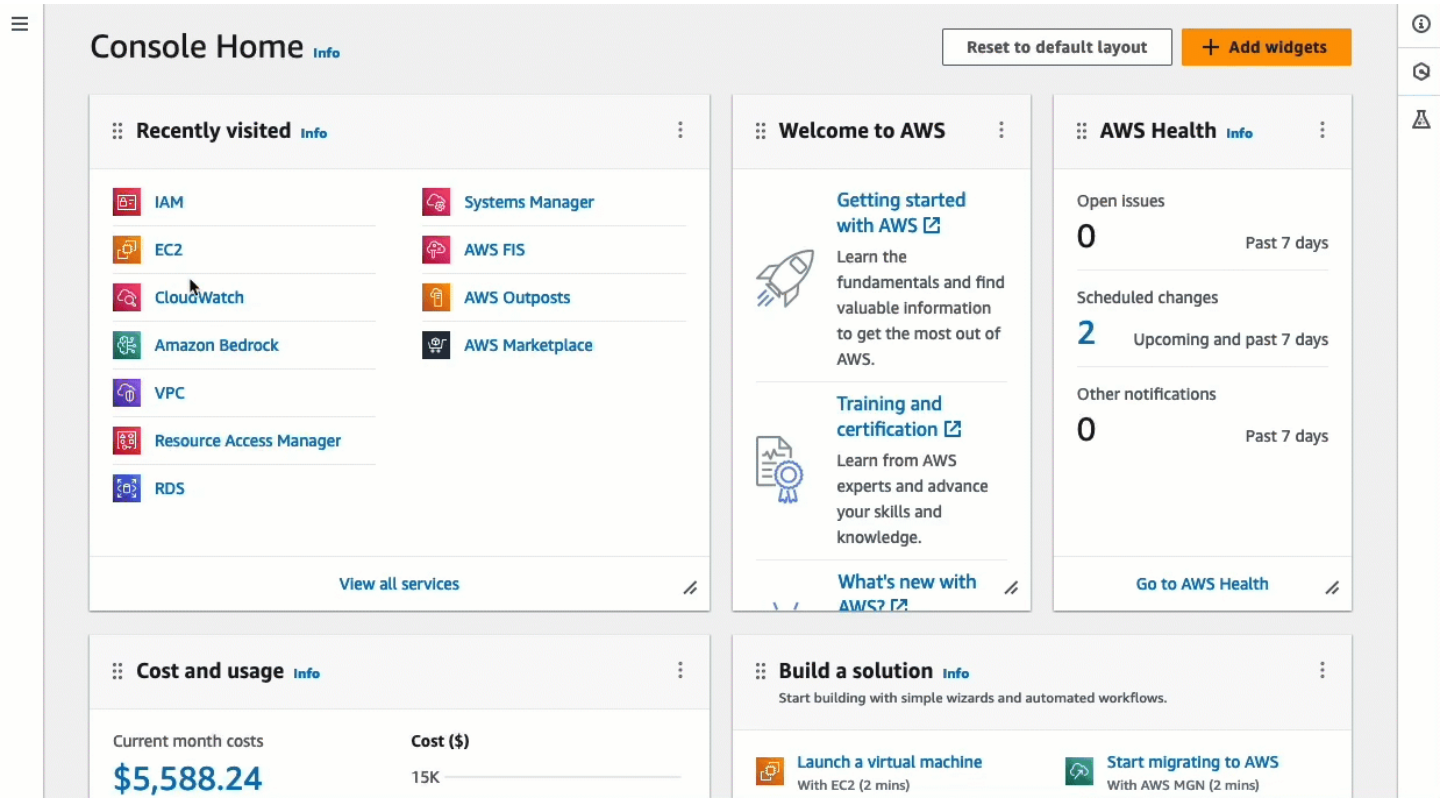
b. En la lista de políticas, seleccione el botón de opción situado junto al nombre de la política que creó. Puede utilizar el cuadro de búsqueda para filtrar la lista de políticas.

c. Elija Acciones, Asociar.

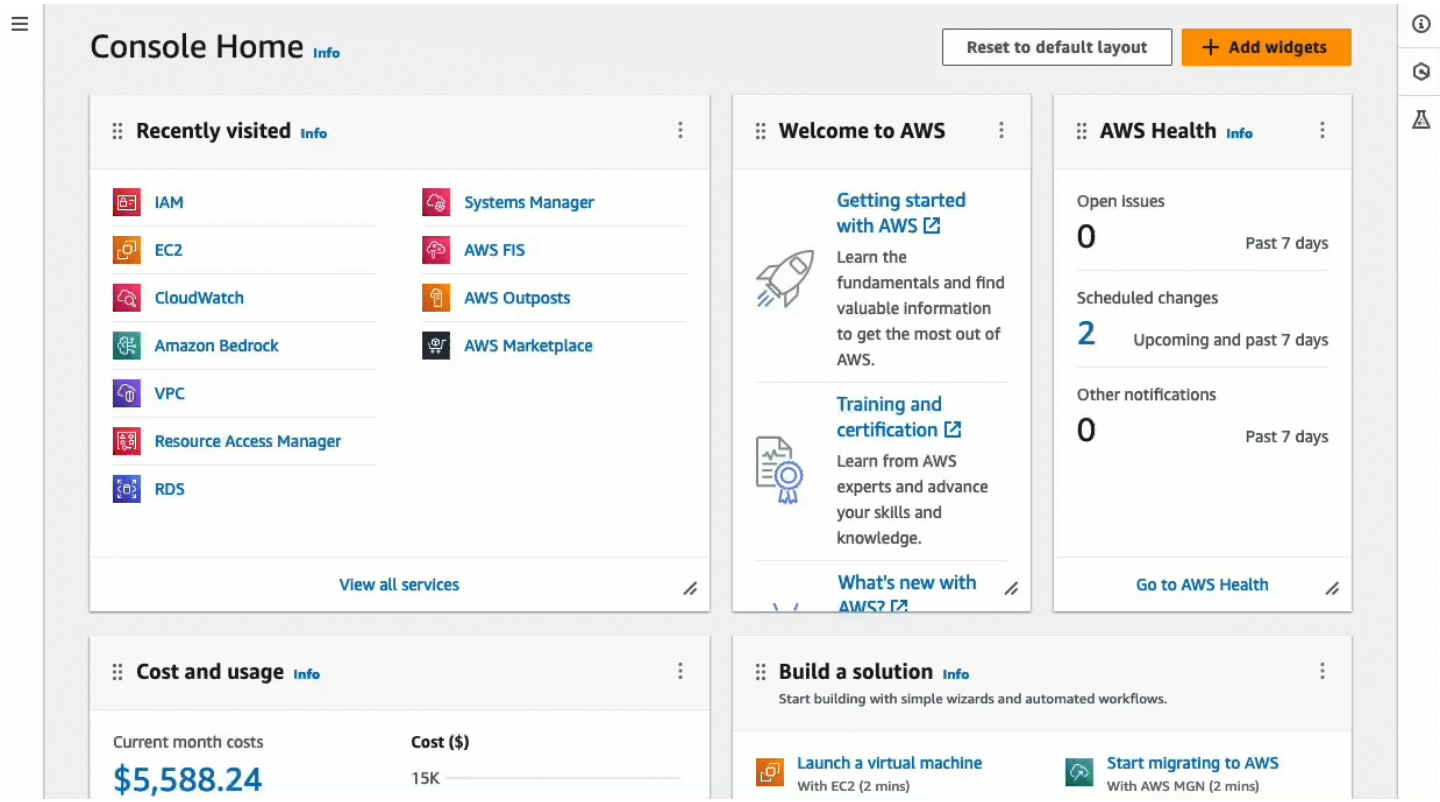
d. En Entidades de IAM, seleccione la casilla de verificación junto a la identidad (usuario, grupo de usuarios o rol). Puede utilizar el cuadro de búsqueda para filtrar la lista de entidades.

e. Elija Asociar política.

Ver una animación: crear una política de IAM



Ver animación: Asociar una política de IAM



Tarea 2: Crear un grupo de seguridad que permita el tráfico entrante desde el servicio EC2 Instance Connect a la instancia

Cuando utiliza EC2 Instance Connect en la consola de Amazon EC2 para conectarse a una instancia, el tráfico que debe permitir que llegue a la instancia es el tráfico desde el servicio EC2 Instance Connect. Esto es diferente a conectarse desde el equipo local a una instancia; en ese caso, debe permitir el tráfico desde el equipo local a la instancia. Para permitir el tráfico desde el servicio EC2 Instance Connect, debe crear un grupo de seguridad que permita el tráfico SSH entrante desde el rango de direcciones IP para el servicio EC2 Instance Connect.

Los rangos de direcciones IP de los servicios de AWS están disponibles en https://ip-ranges.amazonaws.com/ip-ranges.json. Los rangos de direcciones IP de EC2 Instance Connect se identifican mediante `"service": "EC2_INSTANCE_CONNECT"`.

Objetivo de la tarea

En esta tarea, primero encontrará el rango de direcciones IP para `EC2_INSTANCE_CONNECT` en la Región de AWS en la que se encuentra la instancia. Luego deberá crear un grupo de seguridad que permita el tráfico entrante SSH en el puerto 22 de ese rango de direcciones IP.

Pasos para crear el grupo de seguridad

Siga los siguientes pasos para crear un grupo de seguridad. Para ver una animación de los pasos, consulte Ver una animación: obtener el rango de direcciones IP de EC2 Instance Connect para una región específica y Ver una animación: configuración de un grupo de seguridad.

Crear un grupo de seguridad que permita el tráfico entrante desde el servicio EC2 Instance Connect a la instancia

1. Primero, debe obtener el rango de direcciones IP para el servicio EC2 Instance Connect
   a. Abra el archivo JSON de rangos de direcciones IP de AWS en https://ip-ranges.amazonaws.com/ip-ranges.json.
   b. Elija Datos sin procesar.
   c. Busque el rango de direcciones IP para `EC2_INSTANCE_CONNECT` correspondiente a la Región de AWS en la que se encuentra la instancia. Puede usar el campo de búsqueda del navegador para buscar el servicio `EC2_INSTANCE_CONNECT` y continuar hasta encontrar la región en la que se encuentra la instancia.

Por ejemplo, si la instancia está ubicada en la región Este de EE. UU. (Norte de Virginia) (`us-east-1`), el rango de direcciones IP para `EC2_INSTANCE_CONNECT` en esa región es `18.206.107.24/29`.

> **Note**
>
> Los rangos de direcciones IP son diferentes para cada Región de AWS.

d. Copie el rango de direcciones IP que aparece junto a `ip_prefix`. Usará este rango de direcciones IP más tarde en este procedimiento.

Para obtener más información acerca de cómo descargar el archivo JSON de rangos de direcciones IP de AWS y filtrar por servicio, consulte Rangos de direcciones IP de AWS en la Guía del usuario de Amazon VPC.

2. A continuación, cree el grupo de seguridad con una regla de entrada para permitir el tráfico procedente del rango de direcciones IP copiado

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

   b. En el panel de navegación, elija Grupos de seguridad.

   c. Seleccione Crear grupo de seguridad.

   d. En Basic details (Detalles básicos), haga lo siguiente:

      i. En Nombre del grupo de seguridad, ingrese un nombre significativo para el grupo de seguridad.

      ii. En Descripción, escriba una descripción significativa para el grupo de seguridad.

   e. En Reglas de entrada, haga lo siguiente:

      i. Seleccione Agregar regla.

      ii. En Tipo, seleccione SSH.

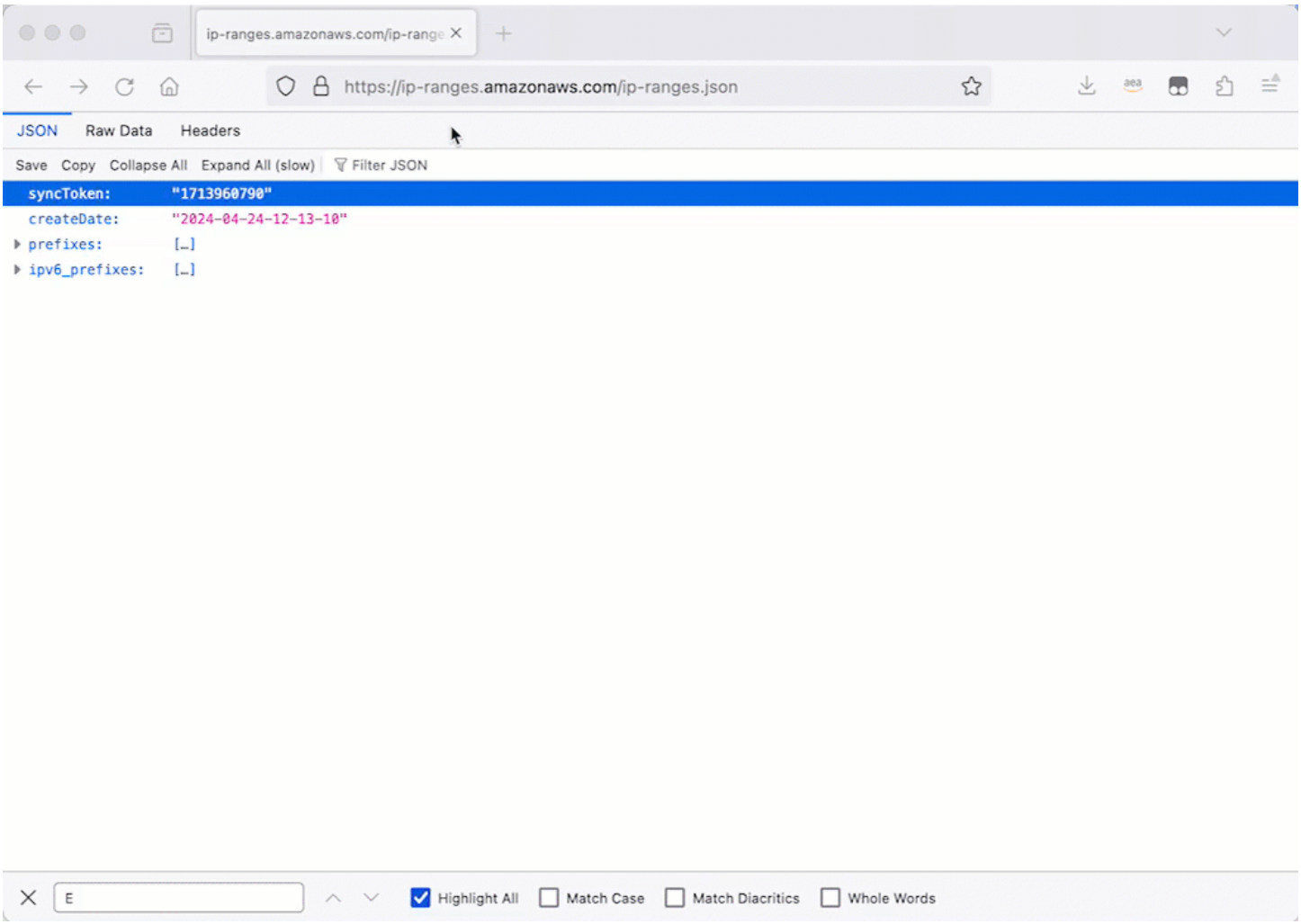
      iii. En Fuente, deje Personalizado.

      iv. En el campo situado junto a Fuente, pegue el rango de direcciones IP del servicio EC2 Instance Connect que copió anteriormente en este procedimiento.

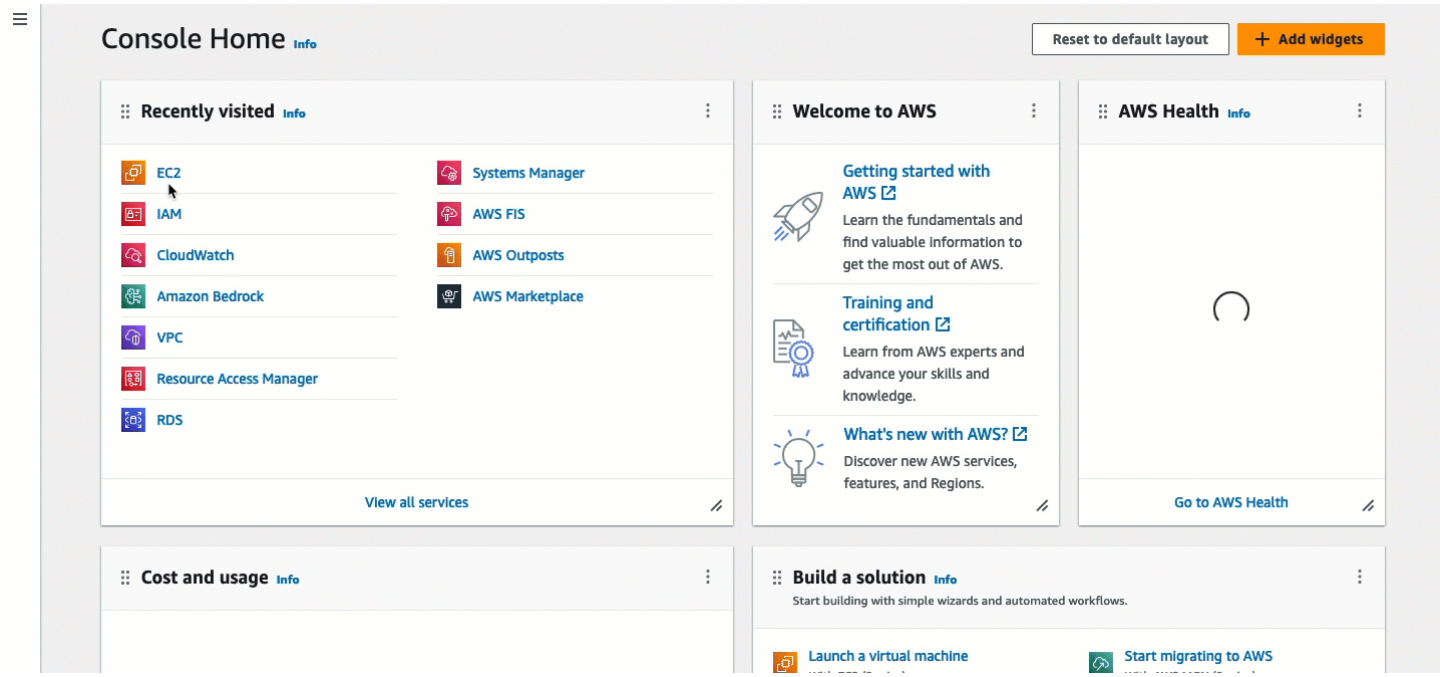
Por ejemplo, si la instancia está ubicada en la región Este de EE. UU. (Norte de Virginia) (`us-east-1`), pegue el siguiente rango de direcciones IP en el campo: `18.206.107.24/29`

f. Elija Crear grupo de seguridad.

Ver una animación: obtener el rango de direcciones IP de EC2 Instance Connect para una región específica



Ver una animación: configuración de un grupo de seguridad



Tarea 3: Iniciar la instancia

Cuando se inicia una instancia, debe especificar una AMI que contenga la información necesaria para lanzar la instancia. Puede elegir iniciar una instancia con o sin EC2 Instance Connect preinstalado. En esta tarea, especificamos una AMI que viene preinstalada con EC2 Instance Connect.

Si inicia la instancia sin EC2 Instance Connect preinstalado y desea usar EC2 Instance Connect para conectarse a la instancia, tendrá que completar pasos de configuración adicionales. Esos pasos están fuera del alcance de este tutorial.

Objetivo de la tarea

En esta tarea, iniciará una instancia con la AMI de Amazon Linux 2023, que viene preinstalada con EC2 Instance Connect. Además, especificará el grupo de seguridad que creó anteriormente para poder usar EC2 Instance Connect en la consola de Amazon EC2 para conectarse a la instancia. Como utilizará EC2 Instance Connect para conectarse a la instancia y, por lo tanto, se introducirá una clave pública en los metadatos de esta, no necesitará especificar una clave SSH cuando inicie dicha instancia. Sin embargo, debe asegurarse de que la instancia tenga una dirección IPv4 pública, ya que el uso de EC2 Instance Connect en la consola de Amazon EC2 solo permite la conexión a instancias con direcciones IPv4 públicas.

Pasos para iniciar una instancia

Siga los pasos que se indican a continuación para iniciar la instancia. Para ver una animación de los pasos, consulte Ver animación: Iniciar la instancia.

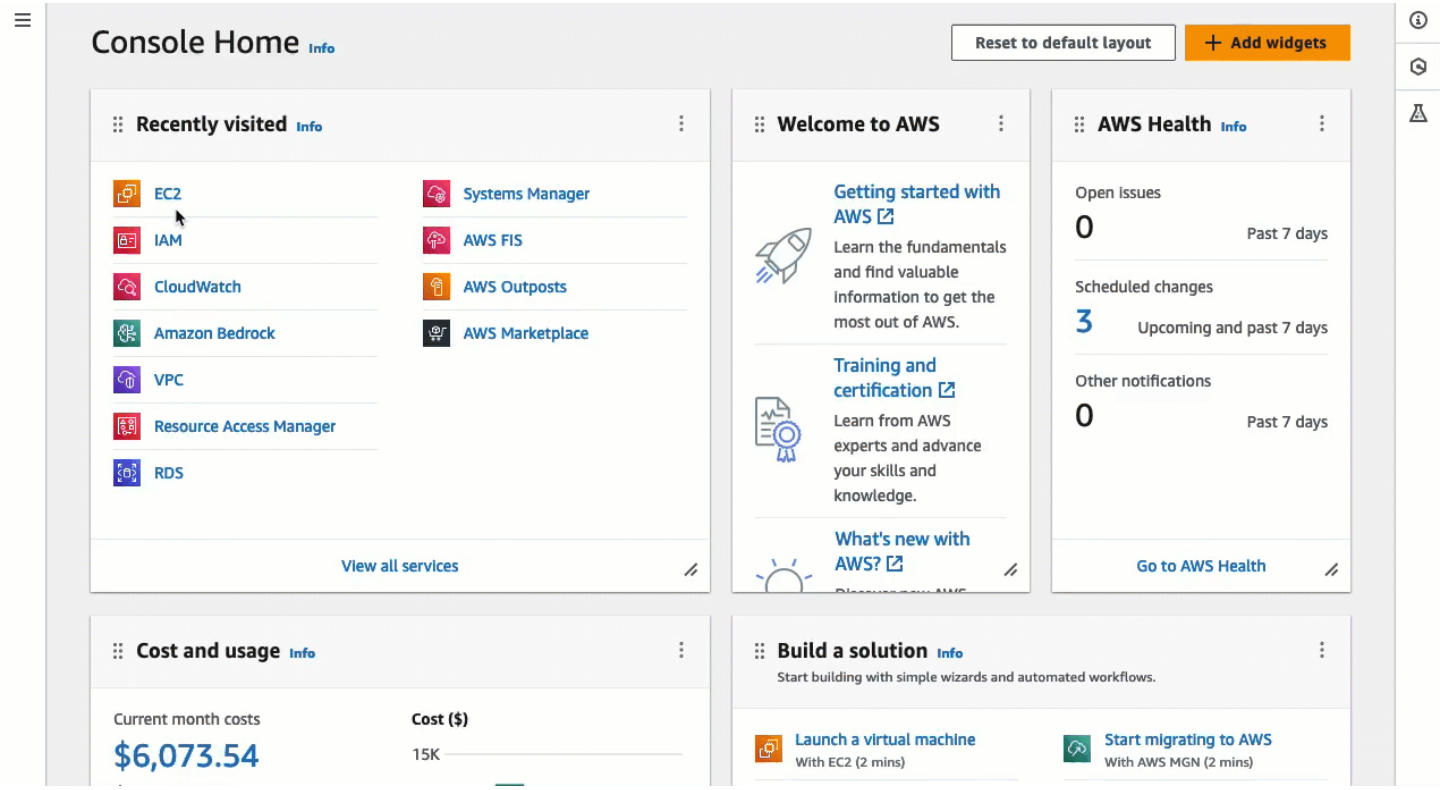
Cómo iniciar una instancia que pueda usar EC2 Instance Connect en la consola de Amazon EC2 para conectarse

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la barra de navegación en la parte superior de la pantalla, se muestra la región actual de AWS (por ejemplo, Irlanda). Seleccione una región en la que se va a iniciar la instancia. Esta elección es importante porque creó un grupo de seguridad que permite el tráfico en una región específica, por lo que debe seleccionar la misma región en la que desea iniciar la instancia.
3. En el panel de la consola de Amazon EC2, elija Iniciar instancia.
4. (Opcional) En Name and tags (Nombre y etiquetas), escriba un nombre descriptivo para la instancia en Name (Nombre).
5. En Imágenes de aplicaciones y SO (Imagen de máquina de Amazon), elija Inicio rápido. Amazon Linux está seleccionado de forma predeterminada. En Imagen de máquina de Amazon (AMI), AMI de Amazon Linux 2023 está seleccionado de forma predeterminada. Mantenga la selección predeterminada para esta tarea.
6. En Tipo de instancia, para Tipo de instancia, mantenga la selección predeterminada o seleccione un tipo de instancia diferente.
7. En Par de claves (inicio de sesión), para Nombre del par de claves, elija Continuar sin un par de claves (no se recomienda). Cuando utiliza EC2 Instance Connect para conectarse a una instancia, EC2 Instance Connect envía un par de claves a los metadatos de la instancia y es este par de claves el que se utiliza para la conexión.
8. En Network settings (Configuración de red), haga lo siguiente:
   a. En Autoasignar IP pública, seleccione Habilitar.

      > **Note**
      >
      > Para utilizar EC2 Instance Connect en la consola de Amazon EC2 para conectarse a una instancia, esta debe tener una dirección IPv4 pública.

   b. En Firewall (grupos de seguridad), elija Seleccionar un grupo de seguridad existente.
   c. En Grupos de seguridad habituales, elija el grupo de seguridad que creó anteriormente.
9. En el panel Resumen, elija Iniciar instancia.

Ver animación: Iniciar la instancia



Tarea 4: Conectarse a la instancia

Cuando se conecta a una instancia con EC2 Instance Connect, la API de EC2 Instance Connect inserta una clave pública SSH en los metadatos de la instancia, donde permanece por 60 segundos. El daemon SSH utiliza `AuthorizedKeysCommand` y `AuthorizedKeysCommandUser` para buscar la clave pública en los metadatos de la instancia para su autenticación y la conecta a la instancia.

Objetivo de la tarea

En esta tarea, se conectará a la instancia mediante EC2 Instance Connect en la consola de Amazon EC2. Si completó las tareas 1, 2 y 3 la conexión debería realizarse correctamente.

Pasos para conectarse a la instancia

Los pasos siguientes le permiten conectarse a la instancia. Para ver una animación de los pasos, consulte Ver animación: Conectarse a la instancia.

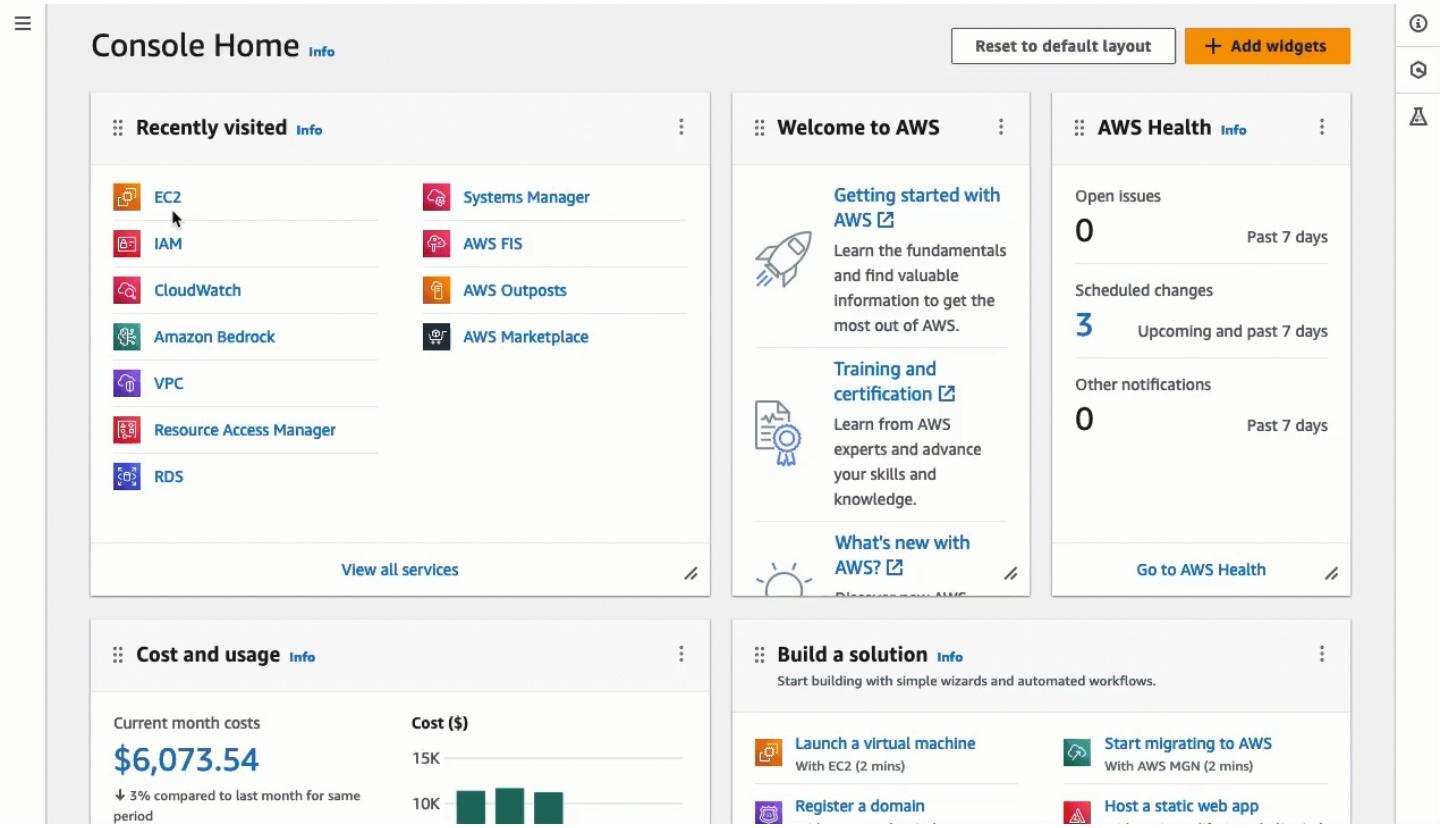
Conectarse a una instancia mediante EC2 Instance Connect en la consola de Amazon EC2

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

2. En la barra de navegación en la parte superior de la pantalla, se muestra la región actual de AWS (por ejemplo, Irlanda). Seleccione la región en la que se encuentra la instancia.
3. En el panel de navegación, seleccione Instances (Instancia[s]).
4. Seleccione la instancia y elija Connect.
5. Elija la pestaña EC2 Instance Connect.
6. En Tipo de conexión, elija Conectarse a una instancia mediante EC2 Instance Connect.
7. Elija Conectar.

   Se abre una ventana terminal en el navegador y está conectado a la instancia.

Ver animación: Conectarse a la instancia



Requisitos previos

Los siguientes son los requisitos previos para instalar EC2 Instance Connect y usarlo para conectarse a una instancia:

- Regiones de AWS
- Zonas locales

- AMI
- Instalación de EC2 Instance Connect
- Dirección IPv4
- Acceso a la red
- Regla del grupo de seguridad
- Concesión de permisos
- Configuración de equipo local
- Nombre de usuario

Regiones de AWS

Se admite en todas las Regiones de AWS, excepto en Oeste de Canadá (Calgary).

Zonas locales

No admitido.

AMI

EC2 Instance Connect viene preinstalado en las siguientes AMI:

- AL2023
- Amazon Linux 2 2.0.20190618 o versiones posteriores
- macOS Sonoma 14.2.1 o posterior
- macOS Ventura 13.6.3 o posterior
- macOS Monterey 12.7.2 o posterior
- Ubuntu 20.04 o versiones posteriores

EC2 Instance Connect no está preinstalado en las siguientes AMI, pero puede instalarlo en instancias que se inician con las siguientes AMI:

- Amazon Linux 2 anterior a la versión 2.0.20190618
- CentOS Stream 8 y 9
- macOS Sonoma anterior a 14.2.1, Ventura anterior a 13.6.3 y Monterey anterior a 12.7.2

- Red Hat Enterprise Linux (RHEL) 8 y 9
- Ubuntu 16.04 o 18.04

Instalación de EC2 Instance Connect

Si quiere utilizar EC2 Instance Connect para conectarse a una instancia, esta debe tenerlo instalado. Puede iniciar la instancia con una AMI que viene preinstalada con EC2 Instance Connect o puede instalar este último en instancias que se inicien con AMI compatibles. Para conocer las AMI compatibles, consulte la sección anterior. Para obtener las instrucciones de instalación, consulte Instalación de EC2 Instance Connect en sus instancias de EC2.

Dirección IPv4

La instancia debe tener una dirección IPv4 (pública o privada). EC2 Instance Connect no admite la conexión mediante una dirección IPv6.

Acceso a la red

Las instancias se pueden configurar para permitir a los usuarios conectarse a ellas a través de Internet o mediante la dirección IP privada de la instancia. Debe configurar el siguiente acceso a la red en función del modo en que los usuarios se conecten a la instancia mediante EC2 Instance Connect:

- Si los usuarios se van a conectar a su instancia a través de Internet, entonces la instancia debe tener una dirección IP pública y estar en una subred pública. Para obtener más información, consulte Habilitar acceso a Internet en la Guía del usuario de Amazon VPC.
- Si los usuarios se van a conectar a la instancia a través de la dirección IP privada de la instancia, debe establecer una conectividad de red privada con la VPC, por ejemplo, mediante AWS Direct Connect, AWS Site-to-Site VPN o la interconexión de VPC, para que los usuarios puedan llegar a la dirección IP privada de la instancia.

Si su instancia no tiene una dirección IPv4 pública y prefiere no configurar el acceso a la red como se describe anteriormente, puede considerar un Punto de conexión de EC2 Instance Connect como alternativa a EC2 Instance Connect. El punto de conexión de EC2 Instance Connect le permite conectarse a una instancia mediante SSH o RDP sin necesidad de que la instancia tenga una dirección IPv4 pública. Para obtener más información, consulte Conexión a la instancia de Linux con la consola de Amazon EC2.

Regla del grupo de seguridad

Asegúrese de que el grupo de seguridad asociado con la instancia permite el tráfico SSH entrante en el puerto 22 desde la dirección IP o desde la red. El grupo de seguridad predeterminado de la VPC no permite el tráfico SSH entrante de forma predeterminada. El grupo de seguridad creado por el asistente de inicialización de instancias habilita el tráfico SSH entrante de forma predeterminada. Para obtener más información, consulte Reglas para conectarse a las instancias desde un equipo.

EC2 Instance Connect utiliza rangos de direcciones IP específicos en las conexiones SSH basadas en navegador a la instancia (cuando los usuarios usan la consola de Amazon EC2 para conectarse a una instancia). Si los usuarios van a usar la consola Amazon EC2 para conectarse a una instancia, asegúrese de que el grupo de seguridad asociado a la instancia permita el tráfico SSH entrante desde el rango de direcciones IP para `EC2_INSTANCE_CONNECT`. Para identificar el rango de direcciones, descargue el archivo JSON proporcionado por AWS y, luego, filtre el subconjunto de EC2 Instance Connect, con `EC2_INSTANCE_CONNECT` como valor del servicio. Estos rangos de direcciones IP difieren entre Regiones de AWS. Para obtener más información acerca de cómo descargar el archivo JSON y filtrar por servicio, consulte Rangos de direcciones IP de AWS en la Guía del usuario de Amazon VPC.

Concesión de permisos

Debe conceder los permisos necesarios a todos los usuarios de IAM que usen EC2 Instance Connect para conectarse a una instancia. Para obtener más información, consulte Concesión de permisos de IAM para EC2 Instance Connect.

Configuración de equipo local

Si los usuarios se van a conectar mediante SSH, deben asegurarse de que su equipo local tenga un cliente SSH.

Es muy probable que los equipos locales de los usuarios tengan un cliente SSH instalado de forma predeterminada. Pueden comprobar si tiene un cliente SSH escribiendo ssh en la línea de comandos. Si su equipo local no reconoce el comando, puede instalar un cliente SSH. Para obtener información sobre la instalación de un cliente SSH en Linux o macOS X, consulte http://www.openssh.com. Para obtener más información sobre la instalación de un cliente SSH en Windows 10, consulte OpenSSH en Windows.

No hay necesidad de instalar un cliente SSH en un equipo local si los usuarios solo usan la consola de Amazon EC2 para conectarse a la instancia.

Nombre de usuario

Cuando se utiliza EC2 Instance Connect para conectarse a una instancia, el nombre de usuario debe cumplir los siguientes requisitos:

- Primer carácter: debe ser una letra (`A-Z`, `a-z`), un dígito (`0-9`) o un guion bajo (`_`)
- Caracteres posteriores: pueden ser letras (`A-Z`, `a-z`), dígitos (`0-9`) o los siguientes caracteres: `@ . _ -`
- Longitud mínima: 1 carácter
- Longitud máxima: 31 caracteres

Concesión de permisos de IAM para EC2 Instance Connect

Si quiere conectarse a una instancia con EC2 Instance Connect, debe crear una política de IAM que conceda permisos a los usuarios para las siguientes acciones y condiciones:

- Acción `ec2-instance-connect:SendSSHPublicKey`: concede permiso a un usuario para insertar la clave pública en una instancia.
- Condición `ec2:osuser`: especifica el nombre del usuario de SO que puede enviar la clave pública a una instancia. Utilice el nombre de usuario predeterminado para la AMI que utilizó para lanzar la instancia. El nombre de usuario predeterminado para AL2023 y Amazon Linux 2 es `ec2-user` y para Ubuntu es `ubuntu`.
- Acción `ec2:DescribeInstances`: es necesaria cuando se utiliza la consola de EC2 debido a que el encapsulador la llama. Es posible que los usuarios ya tengan permiso para llamar a esta acción desde otra política.

Considere restringir el acceso a instancias de EC2 específicas. De lo contrario, todas las entidades principales de IAM con permiso para la acción `ec2-instance-connect:SendSSHPublicKey` pueden conectarse a todas las instancias de EC2. Puede restringir el acceso mediante la especificación de ARN de recursos o al usar etiquetas de recurso como claves de condición.

Para obtener más información, consulte Acciones, recursos y claves de condiciones para Amazon EC2 Instance Connect.

Para obtener información acerca de las políticas de IAM, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Concesión de permisos para que los usuarios se conecten a instancias específicas

La siguiente política de IAM concede permiso para conectarse a instancias específicas, identificadas por sus ARN de recursos.

En el siguiente ejemplo de política de IAM, se especifican las siguientes acciones y condiciones:

- La acción `ec2-instance-connect:SendSSHPublicKey` concede a los usuarios permiso para conectarse a dos instancias, especificadas por los ARN del recurso. Para conceder a los usuarios permiso para conectarse a todas las instancias de EC2, sustituya los ARN del recurso por el carácter comodín `*`.
- La condición `ec2:osuser` concede permiso para conectarse a las instancias solo si se especifica *`ami-username`* al conectarse.
- La acción `ec2:DescribeInstances` se especifica para conceder permisos a los usuarios que usarán la consola para conectarse a sus instancias. Si los usuarios solo utilizarán un cliente SSH para conectarse a sus instancias, puede omitir `ec2:DescribeInstances`. Tenga en cuenta que las acciones de la API `ec2:Describe*` no admiten permisos de recursos. Por lo tanto, el carácter comodín `*` es necesario en el elemento `Resource`.

```
{
 "Version": "2012-10-17",
 "Statement": [{
   "Effect": "Allow",
   "Action": "ec2-instance-connect:SendSSHPublicKey",
   "Resource": [
    "arn:aws:ec2:region:account-id:instance/i-1234567890abcdef0",
    "arn:aws:ec2:region:account-id:instance/i-0598c7d356eba48d7"
   ],
   "Condition": {
    "StringEquals": {
     "ec2:osuser": "ami-username"
    }
   }
  },
  {
   "Effect": "Allow",
   "Action": "ec2:DescribeInstances",
   "Resource": "*"
  }
 ]
```

```
}
```

Concesión de permisos para que los usuarios se conecten a instancias con etiquetas específicas

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos basados en etiquetas que pueden asociarse a usuarios y recursos de AWS. Puede utilizar etiquetas de recursos para controlar el acceso a una instancia. Para obtener más información sobre el uso de etiquetas para controlar el acceso a los recursos de AWS, consulte Control de acceso a los recursos de AWS en la Guía del usuario de IAM.

En el siguiente ejemplo de política de IAM, la acción `ec2-instance-connect:SendSSHPublicKey` concede a los usuarios permiso para conectarse a cualquier instancia (lo que se indica mediante el carácter comodín `*` en el ARN del recurso) con la condición de que la instancia tenga una etiqueta de recurso con key=`tag-key` y value=`tag-value`.

La acción `ec2:DescribeInstances` se especifica para conceder permisos a los usuarios que usarán la consola para conectarse a sus instancias. Si los usuarios solo utilizarán un cliente SSH para conectarse a sus instancias, puede omitir `ec2:DescribeInstances`. Tenga en cuenta que las acciones de la API `ec2:Describe*` no admiten permisos de recursos. Por lo tanto, el carácter comodín `*` es necesario en el elemento `Resource`.

```
{
 "Version": "2012-10-17",
 "Statement": [{
   "Effect": "Allow",
   "Action": "ec2-instance-connect:SendSSHPublicKey",
   "Resource": "arn:aws:ec2:region:account-id:instance/*",
   "Condition": {
    "StringEquals": {
     "aws:ResourceTag/tag-key": "tag-value"
    }
   }
  },
  {
   "Effect": "Allow",
   "Action": "ec2:DescribeInstances",
   "Resource": "*"
  }
 ]
}
```

Instalación de EC2 Instance Connect en sus instancias de EC2

Si quiere utilizar EC2 Instance Connect para conectarse a una instancia, esta debe tenerlo instalado.

EC2 Instance Connect viene preinstalado en las siguientes AMI:

- AMI estándar AL2023
- Amazon Linux 2 2.0.20190618 o versiones posteriores
- macOS Sonoma 14.2.1 o posterior
- macOS Ventura 13.6.3 o posterior
- macOS Monterey 12.7.2 o posterior
- Ubuntu 20.04 o versiones posteriores

Si se inició la instancia con una de las AMI de la lista anterior, puede omitir este procedimiento.

> **Note**
>
> Si ha configurado los ajustes `AuthorizedKeysCommand` y `AuthorizedKeysCommandUser` para la autenticación SSH, la instalación de EC2 Instance Connect no los actualizará. En consecuencia, no puede usar EC2 Instance Connect.

Requisitos previos para la instalación de EC2 Instance Connect

- Lance la instancia con una de las siguientes AMI compatibles:

  Amazon Linux 2 anterior a la versión 2.0.20190618

  AMI mínima de AL2023 o AMI optimizada para Amazon ECS

  CentOS Stream 8 y 9

  macOS Sonoma anterior a 14.2.1, Ventura anterior a 13.6.3 y Monterey anterior a 12.7.2

  Red Hat Enterprise Linux (RHEL) 8 y 9

  Ubuntu 16.04 y 18.04

  Si se inició la instancia con una versión posterior de Amazon Linux 2, macOS Sonoma, Ventura o Monterey, o Ubuntu, viene preinstalada con EC2 Instance Connect y puede omitir este paso.

- Verifique los requisitos previos generales para EC2 Instance Connect.

  Para obtener más información, consulte Requisitos previos.

- Verifique los requisitos previos para conectarse a la instancia mediante un cliente SSH en su equipo local.

  Si su equipo local es Linux o macOS, consulte Conéctese a la instancia de Linux desde Linux o macOS mediante SSH.. Si su equipo local es Windows, consulte Requisitos previos.

  Para obtener más información, consulte Requisitos previos para la conexión SSH.

- Obtenga el ID de la instancia.

  Puede obtener el ID de su instancia con la consola de Amazon EC2 (en la columna “Instance ID” [ID de la instancia]). Si lo prefiere, puede usar el comando Describir instancias (AWS CLI) o el comando Obtener instancia de EC2 (AWS Tools for Windows PowerShell).

- Instale un cliente SSH en el equipo local.

  Su equipo local muy probablemente tiene un cliente SSH instalado de forma predeterminada. Puede comprobar si tiene un cliente SSH escribiendo ssh en la línea de comandos. Si su equipo local no reconoce el comando, puede instalar un cliente SSH. Para obtener información sobre la instalación de un cliente SSH en Linux o macOS X, consulte http://www.openssh.com. Para obtener más información sobre la instalación de un cliente SSH en Windows 10, consulte OpenSSH en Windows.

- (Ubuntu) Instale la AWS CLI en su instancia.

  Para instalar EC2 Instance Connect en una instancia de Ubuntu, debe usar la AWS CLI en la instancia. Para obtener más información sobre la instalación de AWS CLI, consulte Instalación de la AWS CLI en la Guía del usuario de AWS Command Line Interface.

Instalación de EC2 Instance Connect

La instalación de EC2 Instance Connect configura el daemon SSH en la instancia.

Use uno de los siguientes procedimientos para instalar EC2 Instance Connect en función del sistema operativo de la instancia.

Amazon Linux 2

Para instalar EC2 Instance Connect en una instancia iniciada con Amazon Linux 2

1. Conéctese a la instancia de mediante SSH.

   Reemplace los valores de ejemplo en el siguiente comando por los suyos. Use el par de claves SSH que se asignó a su instancia cuando la lanzó y el nombre de usuario predeterminado de la AMI que utilizó para lanzar la instancia. Para Amazon Linux 2, el nombre de usuario predeterminado es `ec2-user`.

   ```
   $ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

   Para obtener más información sobre cómo conectarse a la instancia, consulte Conéctese a la instancia de Linux desde Linux o macOS mediante SSH..

2. Instale el paquete EC2 Instance Connect en su instancia.

   ```
   [ec2-user ~]$ sudo yum install ec2-instance-connect
   ```

   Debe ver tres scripts nuevos en la carpeta `/opt/aws/bin/`:

   ```
   eic_curl_authorized_keys
   eic_parse_authorized_keys
   eic_run_authorized_keys
   ```

3. (Opcional) Compruebe que EC2 Instance Connect se haya instalado correctamente en su instancia.

   ```
   [ec2-user ~]$ sudo less /etc/ssh/sshd_config
   ```

   EC2 Instance Connect se instaló correctamente si las líneas `AuthorizedKeysCommand` y `AuthorizedKeysCommandUser` contienen los siguientes valores:

   ```
   AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys %u %f
   AuthorizedKeysCommandUser ec2-instance-connect
   ```

- `AuthorizedKeysCommand` define el script `eic_run_authorized_keys` para que busque las claves en los metadatos de la instancia
- `AuthorizedKeysCommandUser` define al usuario del sistema como `ec2-instance-connect`

> **Note**
>
> Si ya había configurado `AuthorizedKeysCommand` y `AuthorizedKeysCommandUser`, la instalación de EC2 Instance Connect no cambiará los valores y no podrá usar EC2 Instance Connect.

CentOS

Instalar EC2 Instance Connect en una instancia iniciada con CentOS

1. Conéctese a la instancia de mediante SSH.

   Reemplace los valores de ejemplo en el siguiente comando por los suyos. Use el par de claves SSH que se asignó a su instancia cuando la lanzó y el nombre de usuario predeterminado de la AMI que utilizó para lanzar la instancia. Para CentOS, el nombre de usuario predeterminado es `centos` o `ec2-user`.

   ```
   $ ssh -i my_ec2_private_key.pem centos@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

   Para obtener más información sobre cómo conectarse a la instancia, consulte Conéctese a la instancia de Linux desde Linux o macOS mediante SSH..

2. Si utiliza un proxy HTTP o HTTPS, debe establecer las variables de entorno `http_proxy` o `https_proxy` en la sesión de shell actual.

   Si no usa un proxy, puede omitir este paso.

   - Para un servidor proxy HTTP, ejecute los siguientes comandos:

     ```
     $ export http_proxy=http://hostname:port
     $ export https_proxy=http://hostname:port
     ```

- Para un servidor proxy HTTPS, ejecute los siguientes comandos:

```
$ export http_proxy=https://hostname:port
$ export https_proxy=https://hostname:port
```

3. Instale el paquete de EC2 Instance Connect en su instancia con los siguientes comandos.

   Los archivos de configuración de EC2 Instance Connect para CentOS se proporcionan en un paquete de Red Hat Package Manager (RPM), con diferentes paquetes de RPM para CentOS 8 y CentOS 9 y para tipos de instancia que se ejecutan en Intel/AMD (x86_64) o ARM (AArch64).

   Use el bloque de comandos para el sistema operativo y la arquitectura de la CPU.

   - CentOS 8

     Intel/AMD (x86_64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect.rhel8.rpm -o /
tmp/ec2-instance-connect/ec2-instance-connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

     RAM (AArch64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_arm64/ec2-instance-connect.rhel8.rpm -o /
tmp/ec2-instance-connect/ec2-instance-connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

- CentOS 9

  Intel/AMD (x86_64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

  RAM (AArch64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-west-2.amazonaws.com/latest/linux_arm64/ec2-instance-connect.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

  Debería ver los siguientes scripts nuevos en la carpeta `/opt/aws/bin/`:

```
eic_run_authorized_keys
```

4. (Opcional) Compruebe que EC2 Instance Connect se haya instalado correctamente en su instancia.

   - Para CentOS 8:

```
[ec2-user ~]$ sudo less /lib/systemd/system/ssh.service.d/ec2-instance-connect.conf
```

- Para CentOS 9:

```
[ec2-user ~]$ sudo less /etc/ssh/sshd_config.d/60-ec2-instance-connect.conf
```

EC2 Instance Connect se instaló correctamente si las líneas `AuthorizedKeysCommand` y `AuthorizedKeysCommandUser` contienen los siguientes valores:

```
AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys %u %f
AuthorizedKeysCommandUser ec2-instance-connect
```

- `AuthorizedKeysCommand` define el script `eic_run_authorized_keys` para que busque las claves en los metadatos de la instancia
- `AuthorizedKeysCommandUser` define al usuario del sistema como `ec2-instance-connect`

> **Note**
>
> Si ya había configurado `AuthorizedKeysCommand` y `AuthorizedKeysCommandUser`, la instalación de EC2 Instance Connect no cambiará los valores y no podrá usar EC2 Instance Connect.

macOS

Instalar EC2 Instance Connect en una instancia iniciada con macOS

1. Conéctese a la instancia de mediante SSH.

   Reemplace los valores de ejemplo en el siguiente comando por los suyos. Use el par de claves SSH que se asignó a su instancia cuando la lanzó y el nombre de usuario predeterminado de la AMI que utilizó para lanzar la instancia. Para las instancias de macOS, el nombre de usuario predeterminado es `ec2-user`.

   ```
   $ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

Para obtener más información sobre cómo conectarse a la instancia, consulte Conéctese a la instancia de Linux desde Linux o macOS mediante SSH..

2. Actualice Homebrew mediante el siguiente comando. La actualización incluirá el software que Homebrew conoce. El paquete EC2 Instance Connect se proporciona a través de Homebrew en las instancias de macOS. Para obtener más información, consulte Actualizar el sistema operativo y el software en las instancias de Mac.

```
[ec2-user ~]$ brew update
```

3. Instale el paquete EC2 Instance Connect en su instancia. Esto instalará el software y configurará sshd para usarlo.

```
[ec2-user ~]$ brew install ec2-instance-connect
```

Debería ver los siguientes scripts nuevos en la carpeta `/opt/aws/bin/`:

```
eic_run_authorized_keys
```

4. (Opcional) Compruebe que EC2 Instance Connect se haya instalado correctamente en su instancia.

```
[ec2-user ~]$ sudo less /etc/ssh/sshd_config.d/60-ec2-instance-connect.conf
```

EC2 Instance Connect se instaló correctamente si las líneas `AuthorizedKeysCommand` y `AuthorizedKeysCommandUser` contienen los siguientes valores:

```
AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys %u %f
AuthorizedKeysCommandUser ec2-instance-connect
```

- `AuthorizedKeysCommand` define el script `eic_run_authorized_keys` para que busque las claves en los metadatos de la instancia
- `AuthorizedKeysCommandUser` define al usuario del sistema como `ec2-instance-connect`

> **Note**
>
> Si ya había configurado `AuthorizedKeysCommand` y `AuthorizedKeysCommandUser`, la instalación de EC2 Instance Connect no cambiará los valores y no podrá usar EC2 Instance Connect.

RHEL

Instalar EC2 Instance Connect en una instancia iniciada con Red Hat Enterprise Linux (RHEL)

1. Conéctese a la instancia de mediante SSH.

   Reemplace los valores de ejemplo en el siguiente comando por los suyos. Use el par de claves SSH que se asignó a su instancia cuando la lanzó y el nombre de usuario predeterminado de la AMI que utilizó para lanzar la instancia. Para RHEL, el nombre de usuario predeterminado es `ec2-user` o `root`.

   ```
   $ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

   Para obtener más información sobre cómo conectarse a la instancia, consulte Conéctese a la instancia de Linux desde Linux o macOS mediante SSH..

2. Si utiliza un proxy HTTP o HTTPS, debe establecer las variables de entorno `http_proxy` o `https_proxy` en la sesión de shell actual.

   Si no usa un proxy, puede omitir este paso.

   - Para un servidor proxy HTTP, ejecute los siguientes comandos:

     ```
     $ export http_proxy=http://hostname:port
     $ export https_proxy=http://hostname:port
     ```

   - Para un servidor proxy HTTPS, ejecute los siguientes comandos:

     ```
     $ export http_proxy=https://hostname:port
     $ export https_proxy=https://hostname:port
     ```

3. Instale el paquete de EC2 Instance Connect en su instancia con los siguientes comandos.

   Los archivos de configuración de EC2 Instance Connect para RHEL se proporcionan en un paquete Red Hat Package Manager (RPM), con diferentes paquetes RPM para RHEL 8 y RHEL 9 y, por ejemplo, tipos que se ejecutan en Intel/AMD (x86_64) o ARM (AArch64).

   Use el bloque de comandos para el sistema operativo y la arquitectura de la CPU.

   - RHEL 8

     Intel/AMD (x86_64)

     ```
     [ec2-user ~]$ mkdir /tmp/ec2-instance-connect
     [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect.rhel8.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect.rpm
     [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
     [ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
     ```

     RAM (AArch64)

     ```
     [ec2-user ~]$ mkdir /tmp/ec2-instance-connect
     [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-west-2.amazonaws.com/latest/linux_arm64/ec2-instance-connect.rhel8.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect.rpm
     [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
     [ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
     ```

   - RHEL 9

     Intel/AMD (x86_64)

     ```
     [ec2-user ~]$ mkdir /tmp/ec2-instance-connect
     ```

```
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect.rpm -o /tmp/ec2-
instance-connect/ec2-instance-connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

RAM (AArch64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_arm64/ec2-instance-connect.rpm -o /tmp/ec2-
instance-connect/ec2-instance-connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

Debería ver los siguientes scripts nuevos en la carpeta `/opt/aws/bin/`:

```
eic_run_authorized_keys
```

4. (Opcional) Compruebe que EC2 Instance Connect se haya instalado correctamente en su instancia.

   - Para RHEL 8:

     ```
     [ec2-user ~]$ sudo less /lib/systemd/system/ssh.service.d/ec2-instance-
     connect.conf
     ```

   - Para RHEL 9:

     ```
     [ec2-user ~]$ sudo less /etc/ssh/sshd_config.d/60-ec2-instance-connect.conf
     ```

EC2 Instance Connect se instaló correctamente si las líneas `AuthorizedKeysCommand` y `AuthorizedKeysCommandUser` contienen los siguientes valores:

```
AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys %u %f
AuthorizedKeysCommandUser ec2-instance-connect
```

- `AuthorizedKeysCommand` define el script `eic_run_authorized_keys` para que busque las claves en los metadatos de la instancia
- `AuthorizedKeysCommandUser` define al usuario del sistema como `ec2-instance-connect`

> **Note**
>
> Si ya había configurado `AuthorizedKeysCommand` y `AuthorizedKeysCommandUser`, la instalación de EC2 Instance Connect no cambiará los valores y no podrá usar EC2 Instance Connect.

Ubuntu

Para instalar EC2 Instance Connect en una instancia iniciada con Ubuntu 16.04 o una versión posterior

1. Conéctese a la instancia de mediante SSH.

   Reemplace los valores de ejemplo en el siguiente comando por los suyos. Use el par de claves SSH que se asignó a su instancia cuando la lanzó y el nombre de usuario predeterminado de la AMI que utilizó para lanzar la instancia. Para una AMI de Ubuntu, el nombre de usuario es `ubuntu`.

   ```
   $ ssh -i my_ec2_private_key.pem ubuntu@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

   Para obtener más información sobre cómo conectarse a la instancia, consulte Conéctese a la instancia de Linux desde Linux o macOS mediante SSH..

2. (Opcional) Asegúrese de que su instancia tenga la AMI de Ubuntu más reciente.

Ejecute los siguientes comandos para actualizar todos los paquetes de su instancia.

```
ubuntu:~$ sudo apt-get update
```

```
ubuntu:~$ sudo apt-get upgrade
```

3. Instale el paquete EC2 Instance Connect en su instancia.

```
ubuntu:~$ sudo apt-get install ec2-instance-connect
```

Debe ver tres scripts nuevos en la carpeta `/usr/share/ec2-instance-connect/`:

```
eic_curl_authorized_keys
eic_parse_authorized_keys
eic_run_authorized_keys
```

4. De forma opcional, compruebe que Instance Connect se ha instalado correctamente en su instancia.

```
ubuntu:~$ sudo less /lib/systemd/system/ssh.service.d/ec2-instance-connect.conf
```

EC2 Instance Connect se instaló correctamente si las líneas `AuthorizedKeysCommand` y `AuthorizedKeysCommandUser` contienen los siguientes valores:

```
AuthorizedKeysCommand /usr/share/ec2-instance-connect/eic_run_authorized_keys %
%u %%f
AuthorizedKeysCommandUser ec2-instance-connect
```

- `AuthorizedKeysCommand` define el script `eic_run_authorized_keys` para que busque las claves en los metadatos de la instancia
- `AuthorizedKeysCommandUser` define al usuario del sistema como `ec2-instance-connect`

> **Note**
>
> Si ya había configurado `AuthorizedKeysCommand` y `AuthorizedKeysCommandUser`, la instalación de EC2 Instance Connect no cambiará los valores y no podrá usar EC2 Instance Connect.

Para obtener más información sobre el paquete de EC2 Instance Connect, consulte aws/aws-ec2-instance-connect-config en el sitio web de GitHub.

Conexión mediante EC2 Instance Connect

Las siguientes instrucciones explican cómo conectarse a la instancia de Linux mediante EC2 Instance Connect.

Decida qué opción de conexión va a utilizar.La opción de conexión que se debe utilizar depende de si la instancia tiene una dirección IPv4 pública:

- Consola de Amazon EC2: para conectarse mediante la consola de Amazon EC2, la instancia debe tener una dirección IPv4 pública.
- Cliente SSH: si la instancia no tiene una dirección IP pública, puede conectarse a la instancia mediante una red privada a través de un cliente SSH. Por ejemplo, puede conectarse desde la misma VPC o a través de una conexión de VPN, puerta de enlace de tránsito o AWS Direct Connect.

EC2 Instance Connect no admite la conexión mediante una dirección IPv6.

> **Tip**
>
> EC2 Instance Connect es una de las opciones para conectarse a la instancia de Linux. Para otras opciones, consulte Conexión con la instancia de Linux. Para conectarse a una instancia de Windows, consulte Conexión con la instancia de Windows de.

Opciones conexión para EC2 Instance Connect

- Conectarse desde la consola de Amazon EC2

- Conexión con su propia clave y cliente SSH
- Conexión mediante la AWS CLI
- Solución de problemas

Conectarse desde la consola de Amazon EC2

Puede conectarse a una instancia mediante la consola de Amazon EC2 al seleccionar la instancia desde la consola y elegir conectarse a través de EC2 Instance Connect. Instance Connect gestiona los permisos y proporciona una conexión exitosa.

Para conectarse mediante la consola de Amazon EC2, la instancia debe tener una dirección IPv4 pública. Antes de conectarse, asegúrese de revisar todos los requisitos previos.

Para conectarse a la instancia mediante el cliente basado en el navegador desde la consola de Amazon EC2

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Seleccione la instancia y elija Connect (Conectar).
4. Elija la pestaña EC2 Instance Connect.
5. En Tipo de conexión, elija Conectarse a una instancia mediante EC2 Instance Connect.
6. En Nombre de usuario, escriba el nombre de usuario.
7. Elija Conectarse para abrir una ventana de terminal.

Conexión con su propia clave y cliente SSH

Puede usar su propia clave SSH y conectarse a su instancia desde el cliente SSH que elija al utilizar la API EC2 Instance Connect. Esto le permite aprovechar la capacidad de Instance Connect de insertar una clave pública en la instancia. Este método de conexión funciona para instancias con direcciones IP públicas y privadas.

Requisitos

- Requisitos para pares de claves
  - Tipos compatibles: RSA (OpenSSH y SSH2) y ED25519.
  - Las longitudes admitidas son 2048 y 4096.

  - Para obtener más información, consulte Crear un par de claves con una herramienta de terceros e importar la clave pública a Amazon EC2.
- Cuando se conecta a una instancia que solo tiene direcciones IP privadas, el equipo local desde el que está iniciando la sesión de SSH debe tener conectividad con el punto de conexión del servicio de EC2 Instance Connect (para enviar la clave pública de SSH a la instancia), así como conectividad de red a la dirección IP privada de la instancia a fin de establecer la sesión de SSH. Se puede acceder al punto de conexión de servicio de EC2 Instance Connect a través de Internet o de una interfaz virtual pública de AWS Direct Connect. Para conectarse a la dirección IP privada de la instancia, puede aprovechar servicios tales como AWS Direct Connect, AWS Site-to-Site VPN o el emparejamiento de VPC.

Antes de conectarse, asegúrese de revisar todos los requisitos previos.

Para conectarse a la instancia mediante su propia clave y cualquier cliente SSH

1. De forma opcional, puede generar claves públicas y privadas SSH.

   Puede generar nuevas claves públicas y privadas SSH, `my_key` y `my_key.pub`, mediante el siguiente comando:

   ```
   ssh-keygen -t rsa -f my_key
   ```

2. Inserte la clave pública SSH en la instancia

   Use el comando send-ssh-public-key para insertar la clave pública SSH en la instancia. Si utilizó AL2023 o Amazon Linux 2 para lanzar la instancia, el nombre de usuario predeterminado de la AMI es `ec2-user`. Si utilizó Ubuntu para lanzar la instancia, el nombre de usuario predeterminado de la AMI es `ubuntu`.

   En el siguiente ejemplo, se inserta la clave pública en la instancia especificada, en la zona de disponibilidad especificada, para autenticar `ec2-user`.

   ```
   aws ec2-instance-connect send-ssh-public-key \
       --region us-west-2 \
       --availability-zone us-west-2b \
       --instance-id i-001234a4bf70dec41EXAMPLE \
       --instance-os-user ec2-user \
       --ssh-public-key file://my_key.pub
   ```

3. Conéctese a la instancia mediante su clave privada

   Use el comando ssh para conectarse a la instancia mediante la clave privada antes de que se elimine la clave pública de los metadatos de la instancia (tiene 60 segundos para ello). Especifique la clave privada que se corresponde con la clave pública, el nombre de usuario predeterminado para la AMI que se usó para lanzar la instancia y el nombre del DNS público de la instancia (si se conecta a través de una red privada, especifique el nombre del DNS o la dirección IP privados). Agregue la opción `IdentitiesOnly=yes` para asegurarse de que solo los archivos en la configuración ssh y la clave especificada se utilizan para la conexión.

   ```
   ssh -o "IdentitiesOnly=yes" -i my_key ec2-
   user@ec2-198-51-100-1.compute-1.amazonaws.com
   ```

Conexión mediante la AWS CLI

Si conoce el ID de la instancia, puede utilizar el comando ec2-instance-connect AWS CLI para conectarse a ella mediante un cliente SSH. Si no se especifica un tipo de conexión, EC2 Instance Connect intentará conectarse automáticamente a la dirección IPv4 pública de la instancia. Si la instancia no tiene una dirección IPv4 pública, EC2 Instance Connect intentará conectarse a la dirección IPv4 privada de la instancia a través de un punto de conexión de EC2 Instance Connect. Si la instancia no tiene una dirección IPv4 privada o la VPC no tiene un punto de conexión de EC2 Instance Connect, la instancia de EC2 intentará conectarse a la dirección IPv6 de su instancia.

> **Important**
>
> Antes de conectarse con este método, asegúrese de que ha configurado la AWS CLI, incluidas las credenciales que utiliza; además, confirme que usa la versión más reciente de la AWS CLI. Para obtener más información, consulte Instalación o actualización de la versión más reciente de AWS CLI y Configuración de AWS CLI en la Guía del usuario de AWS Command Line Interface.

Tipos de conexión

`auto` (predeterminado)

La CLI intenta conectarse mediante las direcciones IP de la instancia en el siguiente orden y con el tipo de conexión correspondiente:

- IPv4 pública: `direct`
- IPv4 privada: `eice`
- IPv6: `direct`

`direct`

La CLI se intenta conectar mediante las direcciones IP de la instancia en el siguiente orden (no se conecta a través de un punto de conexión de EC2 Instance Connect):

- IPv4 pública
- IPv6
- IPv4 privada

`eice`

La CLI siempre usa la dirección IPv4 privada de la instancia.

> **Note**
>
> En el futuro, es posible que cambiemos el comportamiento del tipo de conexión `auto`. Para asegurarse de que se utiliza el tipo de conexión deseado, le recomendamos que defina `--connection-type` en `direct` o `eice`.

Cuando se conecta a una instancia con EC2 Instance Connect, la API de EC2 Instance Connect inserta una clave pública SSH en los metadatos de la instancia, donde permanece por 60 segundos. La política de IAM asociada a su usuario le autoriza a insertar la clave pública en los metadatos de la instancia.

Para conectarse a una instancia mediante el ID de la instancia

Si solo conoce el ID de la instancia y quiere que EC2 Instance Connect determine el tipo de conexión que se utilizará al conectarse a la instancia, utilice la CLI de ec2-instance-connect y especifique el parámetro `ssh` y el ID de la instancia.

```
aws ec2-instance-connect ssh --instance-id i-1234567890example
```

> **Tip**
>
> Si aparece un error al usar este comando, asegúrese de que usa la AWS CLI versión 2. El parámetro `ssh` solo está disponible para la AWS CLI versión 2. Para obtener más información, consulte Información AWS CLI sobre la versión 2 en la AWS Command Line InterfaceGuía del usuario.

Para conectarse a una instancia mediante el ID de instancia y un punto de conexión de EC2 Instance Connect

Si quiere conectarse a la instancia a través de un punto de conexión de EC2 Instance Connect, utilice el comando anterior y especifique también el parámetro `--connection-type` con el valor `eice`.

```
aws ec2-instance-connect ssh --instance-id i-1234567890example --connection-type eice
```

Para conectarse a una instancia mediante el ID de la instancia y su propio archivo de clave privada

Si quiere conectarse a la instancia a través de un punto de conexión de EC2 Instance Connect mediante su propia clave privada, especifique el ID de la instancia y la ruta al archivo de clave privada. No incluya *`file://`* en la ruta; se producirá un error en el siguiente ejemplo: *`file:///path/to/key`*.

```
aws ec2-instance-connect ssh --instance-id i-1234567890example --private-key-file /
path/to/key.pem
```

Solución de problemas

Si aparece un error mientras intenta conectarse a la instancia, consulte lo siguiente:

- Solución de problemas de conexión a la instancia de Linux
- ¿Cómo puedo solucionar problemas de conexión a mi instancia de EC2 mediante EC2 Instance Connect?

Desinstalación de EC2 Instance Connect

Para deshabilitar EC2 Instance Connect, conéctese a su instancia y desinstale el paquete `ec2-instance-connect` instalado en el SO. Si la configuración de `sshd` coincide con lo que se definió

cuando instaló EC2 Instance Connect, la desinstalación de `ec2-instance-connect` también elimina la configuración de `sshd`. Si modificó la configuración de `sshd` después de instalar EC2 Instance Connect, debe actualizarla manualmente.

Amazon Linux

Puede desinstalar EC2 Instance Connect en AL2023 y Amazon Linux 2 2.0.20190618 o una versión posterior, donde EC2 Instance Connect está preconfigurado.

Para desinstalar EC2 Instance Connect en una instancia iniciada con Amazon Linux 2

1. Conéctese a la instancia de mediante SSH. Especifique el par de claves SSH que utilizó para su instancia cuando la lanzó y el nombre de usuario predeterminado para la AMI de AL2023 o Amazon Linux 2, que es `ec2-user`.

   Por ejemplo, el siguiente comando ssh conecta a la instancia con el nombre de DNS público `ec2-a-b-c-d.us-west-2.compute.amazonaws.com`, mediante el par de claves `my_ec2_private_key.pem`.

   ```
   $ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

2. Desinstale el paquete `ec2-instance-connect` mediante el comando yum.

   ```
   [ec2-user ~]$ sudo yum remove ec2-instance-connect
   ```

Ubuntu

Para desinstalar EC2 Instance Connect en una instancia iniciada con una AMI de Ubuntu

1. Conéctese a la instancia mediante SSH. Especifique el par de claves SSH que utilizó para su instancia cuando lo lanzó y el nombre de usuario predeterminado para la AMI de Ubuntu, que es `ubuntu`.

   Por ejemplo, el siguiente comando ssh conecta a la instancia con el nombre de DNS público `ec2-a-b-c-d.us-west-2.compute.amazonaws.com`, mediante el par de claves `my_ec2_private_key.pem`.

```
$ ssh -i my_ec2_private_key.pem ubuntu@ec2-a-b-c-d.us-
west-2.compute.amazonaws.com
```

2. Desinstale el paquete `ec2-instance-connect` mediante el comando apt-get.

```
ubuntu:~$ sudo apt-get remove ec2-instance-connect
```

Conexión con la instancia de Windows de

Puede conectarse mediante el escritorio remoto a las instancias de Amazon EC2 creadas a partir de la mayoría de las Imágenes de máquina de Amazon (AMI) de Windows. El escritorio remoto utiliza Remote Desktop Protocol (RDP) para conectarse con la instancia y utilizarla del mismo modo en el que utiliza un ordenador de escritorio (ordenador local). Está disponible en la mayoría de las ediciones de Windows y también para Mac OS.

La licencia del sistema operativo Windows Server permite dos conexiones remotas simultáneas para fines administrativos. La licencia de Windows Server está incluida en el precio de la instancia de Windows. Si necesita más de dos conexiones remotas simultáneas, debe comprar una licencia de Remote Desktop Services (RDS). Si intenta realizar una tercera conexión, se produce un error.

> **Tip**
>
> Si necesita conectarse a la instancia para solucionar problemas de arranque, configuración de red y otros problemas para las instancias creadas en el sistema AWS Nitro, puede usar Consola serie de EC2 para instancias de Amazon EC2.

Contenido

Conexión a la instancia de Windows mediante un cliente RDP

En la siguiente sección, se detallan los requisitos previos y el proceso para conectarse a la instancia mediante su dirección IPv4 o IPv6 con un cliente RDP.

Requisitos previos

Debe cumplir los siguientes requisitos previos para conectarse a la instancia de Windows mediante un cliente RDP.

- Instalar un cliente RDP
  - (Windows) Windows incluye un cliente RDP de forma predeterminada. Para verificarlo, escriba mstsc en la ventana del símbolo del sistema. Si el equipo no reconoce este comando, consulte la página de inicio de Windows y busque la descarga de la aplicación del Escritorio remoto de Microsoft.
  - (macOS X) Descargue la aplicación Microsoft Remote Desktop desde la App Store de Mac.
  - (Linux) Use Remmina.
- Busque la clave privada

  Obtenga la ruta completa de la ubicación del archivo `.pem` en su equipo con el par de claves que especificó cuando lanzó la instancia. Para obtener más información, consulte the section called “Identificación del par de claves públicas que se especificó en el lanzamiento”.

  Si no encuentra el archivo de clave privada, consulte

  > Cuando se conecta a una instancia de Windows recién lanzada, la contraseña de la cuenta de administrador se descifra mediante la clave privada del par de claves que se especificó al lanzar la instancia.
  >
  > Si pierde la contraseña del administrador y ya no tiene la clave privada, debe restablecer la contraseña o crear una nueva instancia. Para obtener más información, consulte Restablecer una contraseña de administrador de Windows perdida o vencida. Para ver los pasos para restablecer la contraseña mediante un documento de Systems Manager, consulte Restablecer contraseñas y claves de SSH en instancias EC2 en la Guía del usuario de AWS Systems Manager.
- Habilite el tráfico RDP entrante desde su dirección IP a su instancia

  Asegúrese de que el grupo de seguridad asociado con la instancia permita el tráfico RDP (`port 3389`) entrante desde la dirección IP. El grupo de seguridad predeterminado no permite el tráfico

RDP entrante de forma predeterminada. Para obtener más información, consulte Reglas para conectarse a las instancias desde un equipo.

> **Tip**
>
> Puede crear un punto de conexión de EC2 Instance Connect para conectarse a la instancia de Windows mediante RDP sin necesidad de una dirección IPv4 pública.

Conexión a una instancia de Windows utilizando RDP y su dirección IPv4

Para conectarse a una instancia de Windows, deber recuperar la contraseña inicial de administrador y usar esta contraseña cuando se conecte a la instancia mediante el escritorio remoto. Pasarán unos minutos desde que la instancia se inicia hasta que la contraseña está disponible.

El nombre de usuario predeterminado de la cuenta de administrador depende del idioma del sistema operativo (SO) incluido en la AMI. Para determinar el nombre de usuario correcto, identifique el idioma del sistema operativo de la AMI y, a continuación, elija el nombre de usuario correspondiente. Por ejemplo, en el caso de un sistema operativo en inglés, el nombre de usuario es `Administrator`; en el caso de un sistema operativo en francés, es `Administrateur`; y en el caso de un sistema operativo en portugués, es `Administrador`. Si la versión de un idioma del sistema operativo no tiene un nombre de usuario en el mismo idioma, elija el nombre de usuario `Administrator (Other)`. Para obtener más información, consulte Localized Names for Administrator Account in Windows en el Wiki de Microsoft TechNet.

Si ha unido su instancia a un dominio, puede conectarse a la instancia con las credenciales de dominio que haya definido en AWS Directory Service. En la pantalla de inicio de sesión del escritorio remoto, en lugar de utilizar el nombre del ordenador local y la contraseña generada, utilice el nombre de usuario completo para el administrador (por ejemplo, **`corp.example.com\Admin`**) y la contraseña de esta cuenta.

Si aparece un error al intentar conectarse a la instancia, consulte the section called “El escritorio remoto no puede conectarse al equipo remoto”.

Para conectarse a la instancia de Windows mediante un cliente RDP

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).

3. Seleccione la instancia y, a continuación, elija Connect (Conectar).
4. En la página Conectarse a la instancia, elija la pestaña Cliente de RDP.
5. En Nombre de usuario, elija el nombre de usuario predeterminado de la cuenta de administrador. El nombre de usuario que elija debe coincidir con el idioma del sistema operativo (SO) incluido en la AMI que utilizó para iniciar la instancia. Si no hay ningún nombre de usuario en el mismo idioma que su sistema operativo, elija Administrador (otro).
6. Elija Obtener contraseña.
7. En la página Obtener contraseña de Windows, haga lo siguiente:

   a. Elija Cargar archivo de clave privada y vaya el archivo de clave privada (`.pem`) que especificó al iniciar la instancia. Seleccione el archivo y elija Open (Abrir) para copiar todo el contenido del archivo en esta ventana.

   b. Elija Descifrar contraseña. La página Obtener contraseña de Windows se cierra y la contraseña de administrador predeterminada de la instancia aparece en Contraseña y reemplaza al enlace Obtener contraseña mostrado anteriormente.

   c. Copie la contraseña y guárdela en un lugar seguro. Necesitará la contraseña para conectarse a la instancia.
8. Elija Download remote desktop file (Descargar archivo de escritorio remoto). Cuando haya terminado de descargar el archivo, elija Cancel (Cancelar) para volver a la página Instances (instancia[s]). Desplácese hasta el directorio de descargas y abra el archivo RDP.
9. Es posible que aparezca una advertencia en la que se indique que se desconoce el publicador de la conexión remota. Elija Connect (Conectarse) para conectarse a su instancia.
10. La cuenta de administrador está seleccionada de forma predeterminada. Pegue la contraseña que copió anteriormente y, a continuación, elija OK.
11. Debido a la naturaleza de los certificados autofirmados, es posible que aparezca una advertencia que indica que no se pudo autenticar el certificado de seguridad. Realice una de las siguientes acciones siguientes:

    - Si confía en el certificado, seleccione Sí para conectarse a la instancia.
    - [Windows] Antes de continuar, compare la huella digital del certificado con el valor del registro del sistema para confirmar la identidad del equipo remoto. Elija Ver el certificado y, a continuación, seleccione Huella digital en la pestaña Detalles. Compare este valor con el valor de `RDPCERTIFICATE-THUMBPRINT` en Acciones, Supervisar y solucionar problemas, Obtener el registro del sistema.

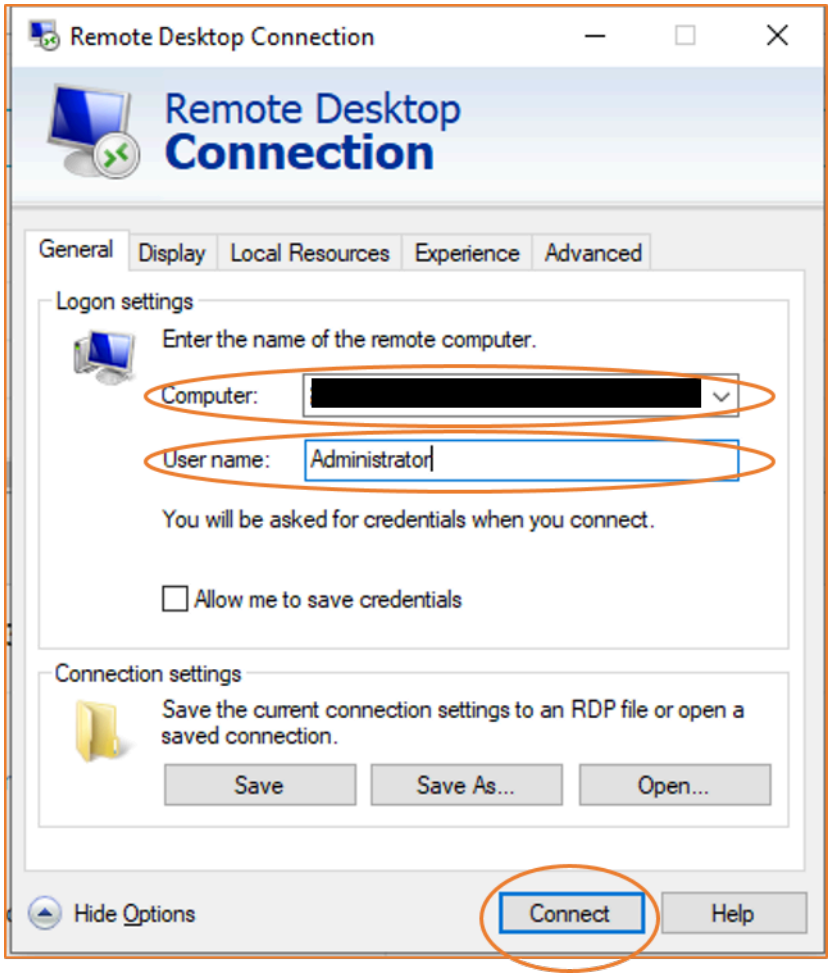
- [Mac OS X] Antes de continuar, compare la huella digital del certificado con el valor del registro del sistema para confirmar la identidad del equipo remoto. Seleccione Mostrar certificado, expanda Detalles y elija Huellas digitales SHA1. Compare este valor con el valor de `RDPCERTIFICATE-THUMBPRINT` en Acciones, Supervisar y solucionar problemas, Obtener el registro del sistema.

Conexión a una instancia de Windows utilizando RDP y su dirección IPv6

Si habilitó la VPC para IPv6 y asignó una dirección IPv6 a la instancia de Windows, puede utilizar un cliente RDP para conectarse a la instancia con la dirección IPv6 (por ejemplo `2001:db8:1234:1a00:9691:9503:25ad:1761`), en lugar de con una dirección IPv4 pública o un nombre de host DNS público.

Para conectarse a la instancia de Windows utilizando su dirección IPv6

1. Obtenga la contraseña de administrador inicial para la instancia, tal y como se describe en Conexión a la instancia de Windows mediante un cliente RDP. Necesitará la contraseña para conectarse a la instancia.
2. (Windows) Abra el cliente RDP en un equipo Windows, elija Mostrar opciones y haga lo siguiente:



- En Computer (Equipo), escriba la dirección IPv6 de la instancia de Windows.
- En User name (Nombre de usuario), escriba Administrator (Administrador).
- Elija Connect.
- Cuando se le solicite, escriba la contraseña que guardó anteriormente.

(macOS X) Abra el cliente RDP en el equipo y haga lo siguiente:

- Elija Nuevo.
- En PC Name (Nombre de equipo), escriba la dirección IPv6 de la instancia de Windows.
- En User name (Nombre de usuario), escriba Administrator (Administrador).
- Cierre el cuadro de diálogo. En My Desktops (Mis escritorios), seleccione la conexión y a continuación,Start (Inicio).
- Cuando se le solicite, escriba la contraseña que guardó anteriormente.

3. Debido a la naturaleza de los certificados autofirmados, es posible que aparezca una advertencia que indica que no se pudo autenticar el certificado de seguridad. Si confía en el certificado, puede seleccionar Yes (Sí) o Continue (Continuar). De lo contrario, puede verificar la identidad del equipo remoto, como se describe en Conexión a la instancia de Windows mediante un cliente RDP.

Conexión a la instancia de Windows mediante Fleet Manager

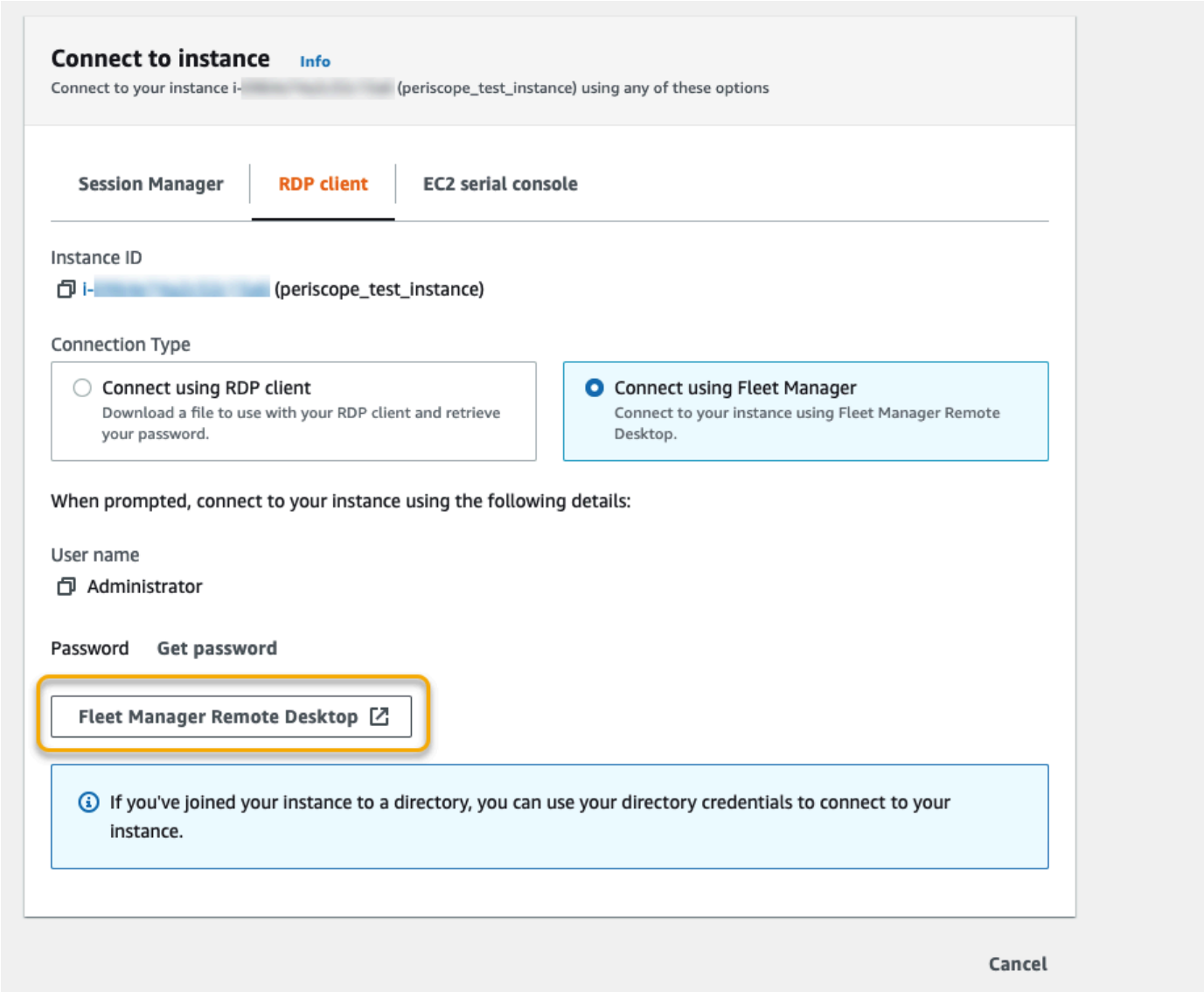
Puede usar Fleet Manager, una función de AWS Systems Manager, para conectarse a instancias de Windows mediante el protocolo de escritorio remoto (RDP) y mostrar hasta cuatro instancias de Windows en la misma página de la AWS Management Console. Puede conectarse a la primera instancia en el escritorio remoto de Fleet Manager directamente desde la página instancias de la consola de Amazon EC2. Para obtener más información sobre Fleet Manager, consulte Conectarse a un nodo administrado mediante el Escritorio remoto en la Guía del usuario de AWS Systems Manager.

Antes de intentar conectarse a una instancia mediante Fleet Manager, asegúrese de que se hayan completado los pasos de configuración necesarios. Para obtener más información, consulte Configuración de Systems Manager.

> **Note**
>
> No necesita permitir específicamente el tráfico RDP entrante de su dirección IP si usa Fleet Manager para conectarse. Fleet Manager se encarga de eso automáticamente.

Conectarse a instancias mediante RDP con Fleet Manager (consola)

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instances (instancia[s]).
3. Seleccione la instancia y, a continuación, elija Connect (Conectar).
4. En la página Connect to instance (Conectarse a la instancia), elija la opción Connect using Fleet Manager (Conectarse mediante Fleet Manager) y, a continuación, elija Fleet Manager Remote Desktop (Escritorio remoto de Fleet Manager). De esta forma, se abre la página Fleet Manager Remote Desktop (Escritorio remoto de Fleet Manager) en la consola de AWS Systems Manager.



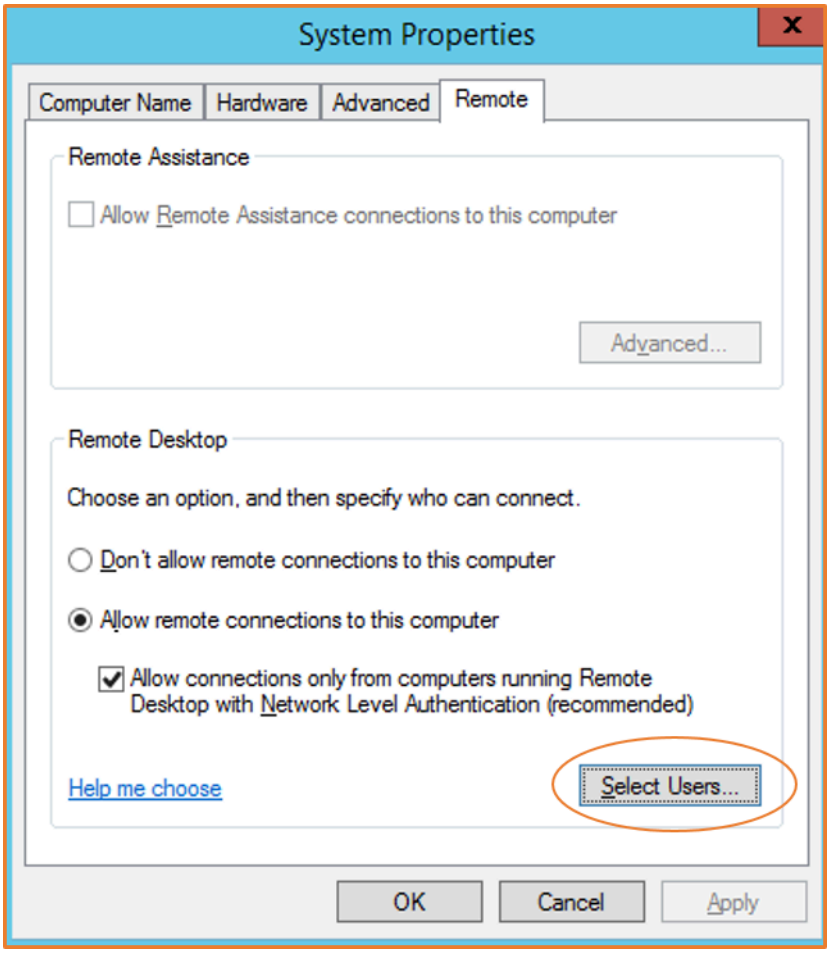
Para obtener más información sobre cómo conectarse a instancias de Windows desde la página Fleet Manager Remote Desktop (Escritorio remoto de Fleet Manager), consulte Connect using Remote Desktop en la Guía del usuario de AWS Systems Manager.

Configurar cuentas

Después de conectarse a través de RDP, recomendamos que realice lo siguiente:

- Cambie la contraseña de administrador del valor predeterminado. Puede cambiar la contraseña mientras se está conectado a la instancia, al igual que en cualquier otro equipo que ejecuta Windows Server.

- Cree otro usuario con privilegios de administrador en la instancia. Esto es una protección en caso de que olvide la contraseña de administrador o tenga un problema con la cuenta de administrador. El usuario nueva debe tener permiso de acceso a la instancia de manera remota. Abra Propiedades del sistema haciendo clic con el botón derecho del ratón en el icono Este equipo en su escritorio de Windows o en el Explorador de archivos y seleccione Propiedades. Elija Configuración de Acceso remoto y elija Seleccionar usuarios para añadir el usuario al grupo Usuarios de escritorio remoto.



Transferencia de archivos a instancias de Windows

Puede trabajar con la instancia de Windows del mismo modo que lo haría con cualquier servidor Windows. Por ejemplo, puede transferir archivos entre instancias de Windows y el equipo local usando la característica para compartir archivos locales del software de Conexión a Escritorio remoto de Microsoft (RDP). Puede obtener acceso a los archivos locales de los discos duros, las unidades de DVD, los dispositivos portátiles y las unidades de red mapeadas.

Para acceder a los archivos locales desde las instancias de Windows, debe habilitar la característica de uso compartido de archivos locales mediante la asignación de la unidad de sesión remota a la unidad local. Los pasos son ligeramente diferentes en función de si el sistema operativo de la computadora local es Windows o macOS X.

Windows

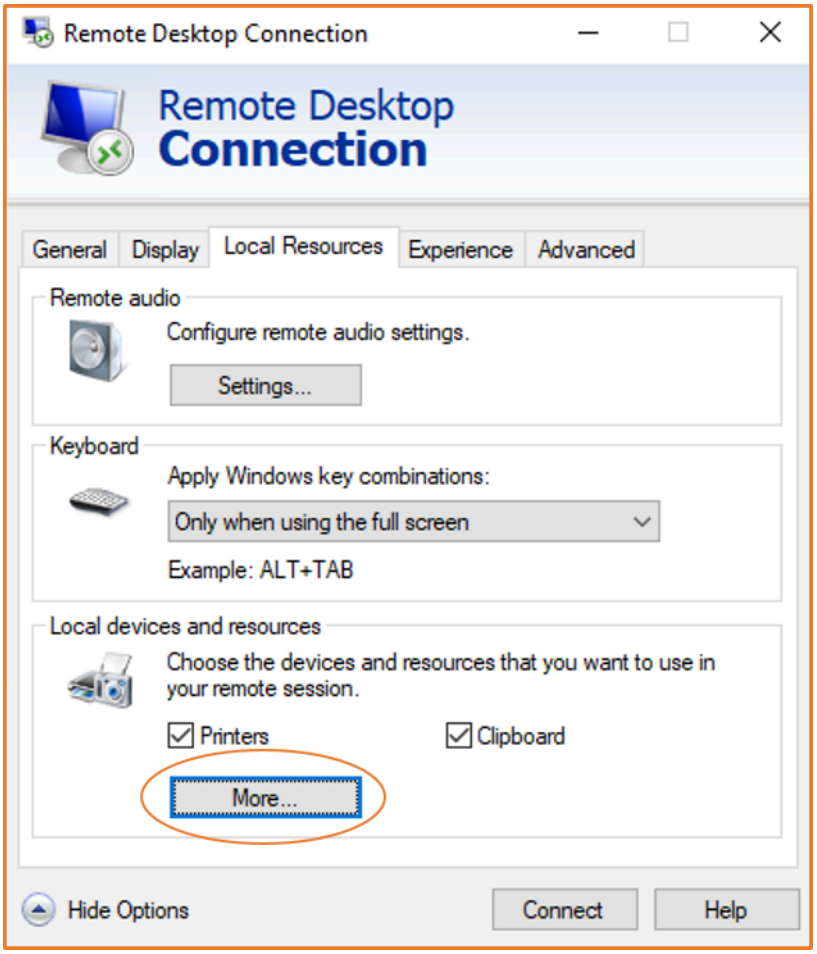
Para asignar la unidad de sesión remota a la unidad local en la computadora Windows local

1. Abra el cliente de conexión al Escritorio remoto.
2. Elija Show Options.
3. Agregue el nombre de host de la instancia en el campo Computer (Computadora) y el nombre del usuario en el campo User name (Nombre de usuario), como se indica a continuación:

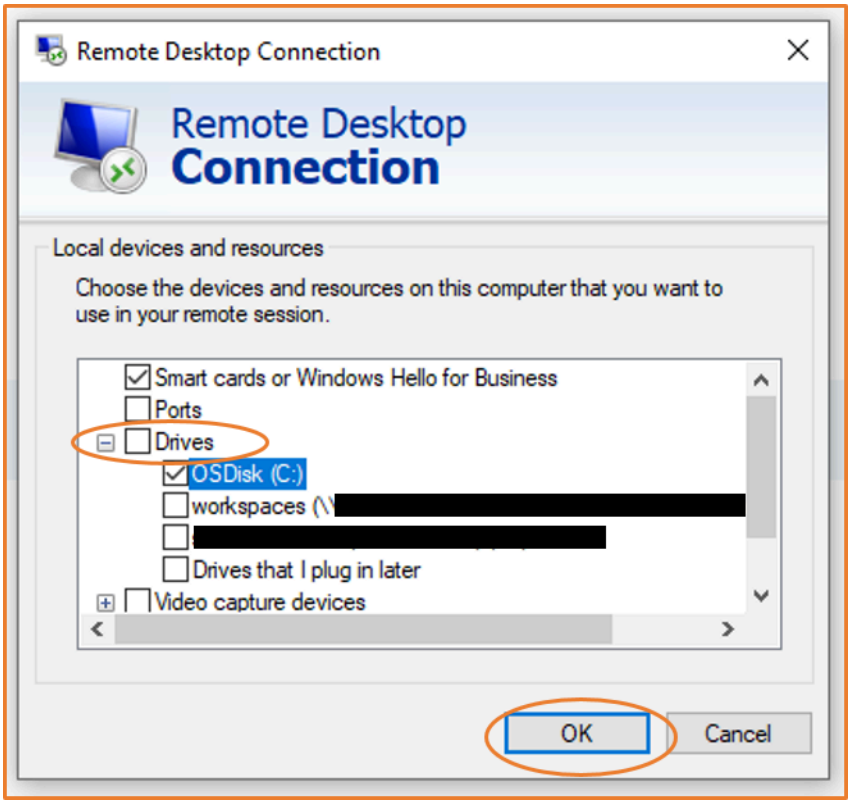
   a. En Connection settings (Configuración de conexión), elija Open… (Abrir…) y diríjase al archivo de acceso directo RDP que descargó de la consola de Amazon EC2. El archivo contiene el nombre de host del DNS IPv4 público, que identifica la instancia y el nombre de usuario del administrador.

   b. Seleccione el archivo y elija Open (Abrir). Los campos Computer (Computadora) y User name (Nombre de usuario) se completan con los valores del archivo de acceso directo RDP.

   c. Seleccione Guardar.
4. Elija la pestaña Local Resources (Recursos locales).
5. En Local Devices and resources (Dispositivos y recursos locales), elija More... (Más...)



6. Abra Drives (Unidades) y seleccione la unidad local que desea asignar a su instancia de Windows.
7. Seleccione OK.

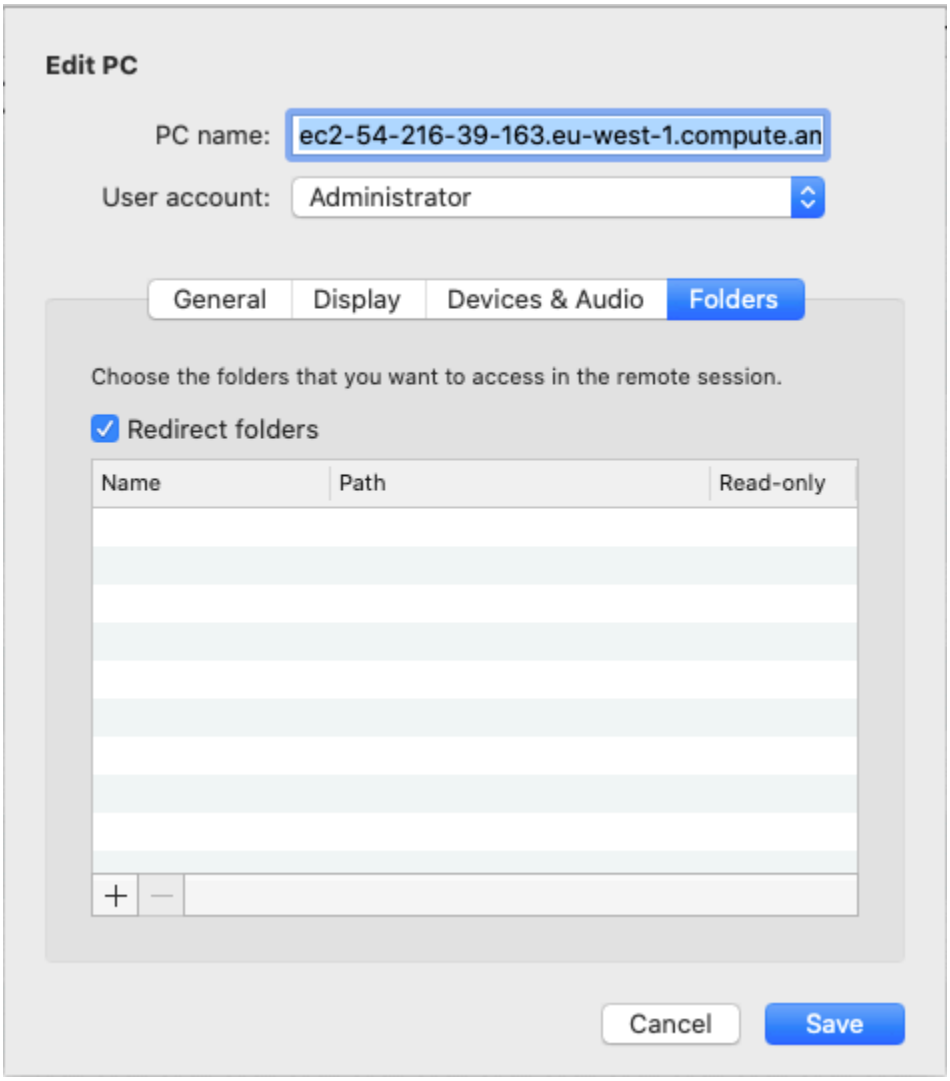


8. Seleccione Conectar para conectarse a su instancia de Windows.

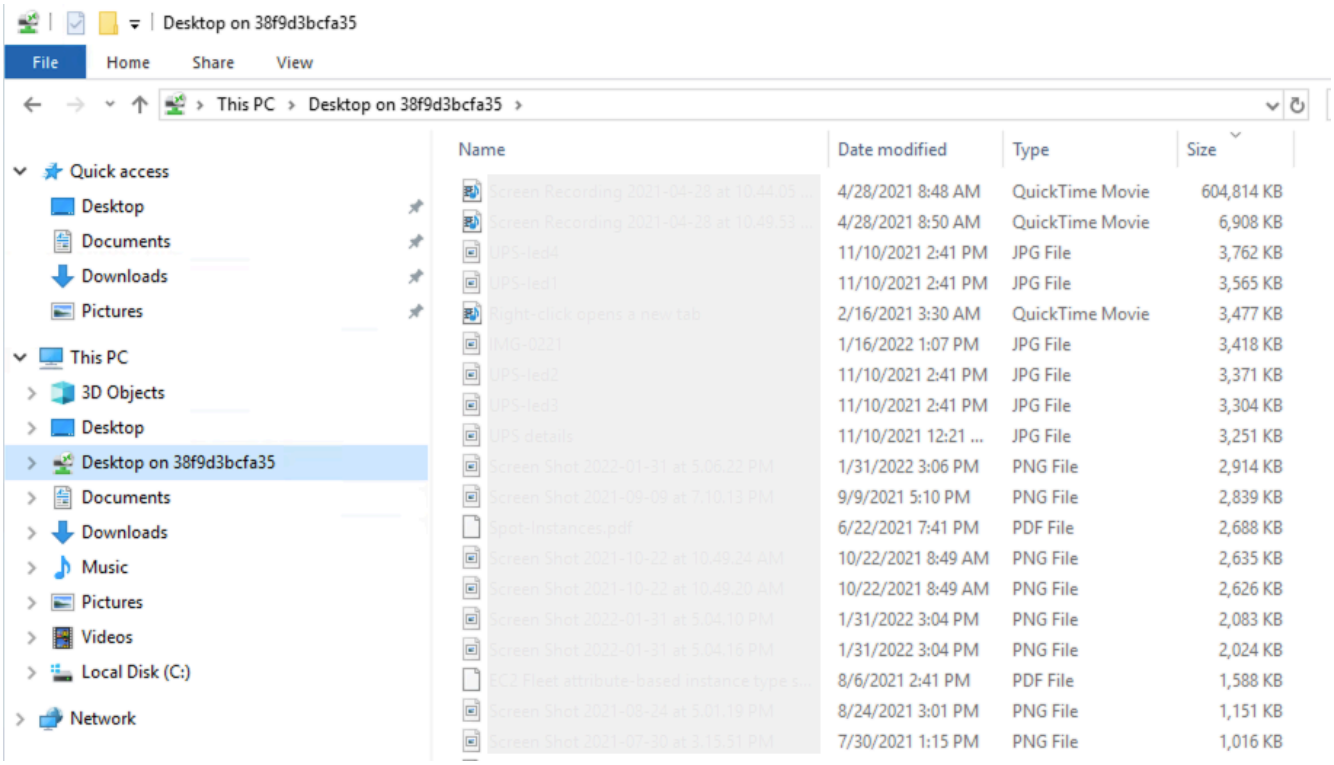
macOS X

Para asignar la unidad de sesión remota a la carpeta local en la computadora macOS X local

1. Abra el cliente de conexión al Escritorio remoto.
2. Diríjase al archivo RDP que descargó de la consola de Amazon EC2 (cuando se conectó inicialmente a la instancia) y arrástrelo al cliente de conexión a escritorio remoto.
3. Haga clic con el botón derecho en el archivo RDP y elija Edit (Editar).
4. Elija la pestaña Folders (Carpetas) y seleccione la casilla Redirect folders (Redirigir carpetas).



5. Elija el icono + en la parte inferior izquierda, diríjase a la carpeta que desea asignar y elija Open (Abrir). Repita este paso para cada carpeta que desee asignar.
6. Seleccione Guardar.
7. Seleccione Conectar para conectarse a su instancia de Windows. Se le pedirá la contraseña.
8. En la instancia, en el explorador de archivos, expanda This PC (Esta PC) y busque la carpeta compartida desde la que puede acceder a los archivos locales. En la siguiente captura de pantalla, la carpeta Desktop (Escritorio) de la computadora local se asignó a la unidad de sesión remota de la instancia.



Para obtener más información sobre cómo hacer que los dispositivos locales estén disponibles para una sesión remota en una computadora Mac, consulte Get started with the macOS client (Introducción a cliente de macOS).

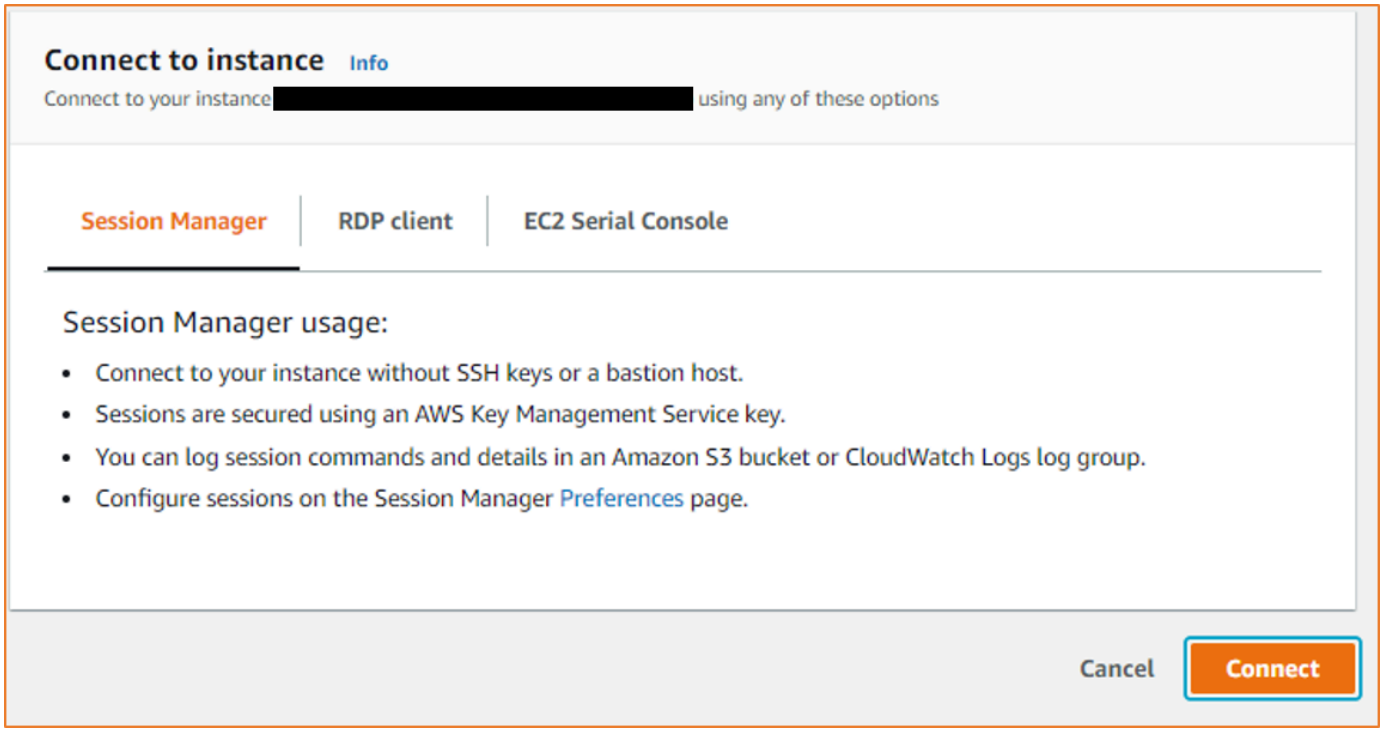
Conexión mediante el Administrador de sesiones

El Administrador de sesiones es una funcionalidad de AWS Systems Manager completamente administrada que permite administrar las instancias de Amazon EC2 a través de un shell interactivo basado en navegador con un solo clic o a través de la AWS CLI. Puede utilizar el Administrador de sesiones para iniciar una sesión con una instancia en su cuenta. Después de iniciar la sesión, puede ejecutar comandos interactivos en la instancia como lo haría a través de cualquier otro tipo de conexión. Para obtener más información acerca del Administrador de sesiones, consulte Administrador de sesiones de AWS Systems Manager en la Guía del usuario de AWS Systems Manager.

Antes de intentar conectarse a una instancia mediante el Administrador de sesiones, asegúrese de que haya completado los pasos de configuración necesarios. Para obtener más información, consulte Configuración de Session Manager.

Para conectarse a una instancia de Amazon EC2 mediante el Administrador de sesiones en la consola de Amazon EC2

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Seleccione la instancia y elija Connect (Conectar).
4. En Connection method (Método de conexión), elija Session Manager (Administrador de sesiones).
5. Elija Conectar.



> **Tip**
>
> Si recibe un error que indica que no está autorizado a realizar una o más acciones de Administrador de sistemas (`ssm:command-name`), debe actualizar las políticas para que le permitan iniciar sesiones desde la consola de Amazon EC2. Para obtener más información e instrucciones, consulte Políticas de IAM predeterminadas de inicio rápido para el Administrador de sesiones en la Guía del usuario de AWS Systems Manager.

Conexión a las instancias mediante el punto de conexión de EC2 Instance Connect

El punto de conexión de EC2 Instance Connect le permite conectarse de forma segura a una instancia desde Internet, sin utilizar un host bastión ni requerir que su nube privada virtual (VPC) tenga conectividad directa a Internet.

Ventajas

- Ahora puede conectarse a sus instancias sin que estas tengan una dirección IPv4 pública. AWS cobra por todas las direcciones IPv4 públicas, incluidas las direcciones IPv4 públicas asociadas a las instancias en ejecución y las direcciones IP elásticas. Para obtener más información, consulte la pestaña Dirección IPv4 pública en la página Precios de Amazon VPC.
- Puede conectarse a las instancias desde Internet sin necesidad de que su VPC tenga conectividad directa a Internet mediante una puerta de enlace de Internet.
- Puede controlar el acceso a la creación y el uso de los puntos de conexión de EC2 Instance Connect para conectarse a las instancias con permisos y políticas de IAM.
- Todos los intentos de conexión a las instancias, tanto los correctos como los que producen errores, se registran en CloudTrail.

Precios

El uso de los puntos de conexión de EC2 Instance Connect no conlleva ningún costo adicional. Si utiliza un punto de conexión de EC2 Instance Connect para conectarse a una instancia que se encuentra en una zona de disponibilidad diferente, se aplica un cargo adicional por transferencia de datos entre zonas de disponibilidad.

Contenido

- Registro de las conexiones establecidas en el punto de conexión de EC2 Instance Connect
- Eliminar un punto de conexión de EC2 Instance Connect
- Rol vinculado a un servicio del punto de conexión de EC2 Instance Connect
- Cupo del Punto de conexión de EC2 Instance Connect

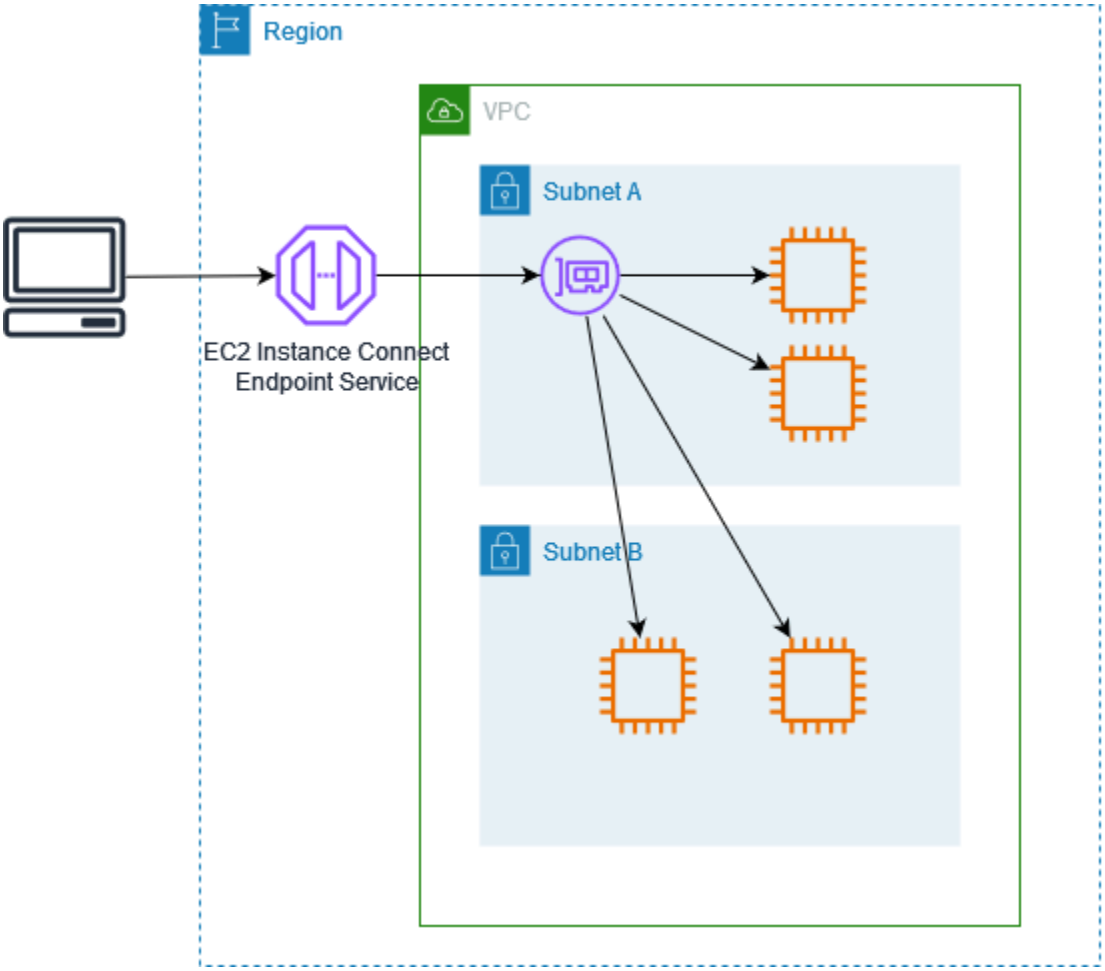
Funcionamiento

El punto de conexión de EC2 Instance Connect es un proxy TCP que reconoce la identidad. El servicio de punto de conexión de EC2 Instance Connect establece un túnel privado desde el equipo hasta el punto final mediante las credenciales de la entidad de IAM. El tráfico se autentica y autoriza antes de que llegue a la VPC.

Puede configurar reglas de grupos de seguridad adicionales para restringir el tráfico entrante a las instancias. Por ejemplo, puede usar reglas de entrada en las instancias para permitir únicamente el tráfico en los puertos de administración desde el punto de conexión de EC2 Instance Connect.

Puede configurar las reglas de la tabla de enrutamiento para permitir que el punto de conexión se conecte a cualquier instancia de cualquier subred de la VPC.

En el siguiente diagrama, se muestra cómo un usuario puede conectarse a las instancias desde Internet mediante un punto de conexión de EC2 Instance Connect. En primer lugar, cree un punto de conexión de EC2 Instance Connect en la subred A. Creamos una interfaz de red para el punto de conexión en la subred, que sirve como punto de entrada para el tráfico destinado a las instancias de la VPC. Si la tabla de enrutamiento de la subred B permite el tráfico de la subred A, puede usar el punto de conexión para llegar a las instancias de la subred B.



Consideraciones

Antes de comenzar, considere lo siguiente:

- El punto de conexión de EC2 Instance Connect está diseñado específicamente para casos de uso de tráfico de administración y no para transferencias de datos de gran volumen. Las transferencias de datos de gran volumen están limitadas.
- La instancia debe tener una dirección IPv4 (pública o privada). El punto de conexión de EC2 Instance Connect no admite la conexión a instancias mediante direcciones IPv6.
- (Instancias de Linux) Si usa su propio par de claves, puede usar cualquier AMI de Linux. De lo contrario, la instancia debe tener instalado EC2 Instance Connect. Para obtener información sobre qué AMI incluyen EC2 Instance Connect y cómo instalarlo en otras AMI compatibles, consulte Instalación de EC2 Instance Connect.
- Puede asignar un grupo de seguridad a un punto de conexión de EC2 Instance Connect cuando lo cree. De lo contrario, se usará el grupo de seguridad predeterminado para la VPC. El grupo de

seguridad de un punto de conexión de EC2 Instance Connect debe permitir el tráfico saliente a las instancias de destino. Para obtener más información, consulte Grupos de seguridad para el punto de conexión de EC2 Instance Connect.

- Puede configurar un punto de conexión de EC2 Instance Connect para mantener las direcciones IP de origen de los clientes al enrutar las solicitudes a las instancias. De lo contrario, la dirección IP de la interfaz de red pasará a ser la dirección IP del cliente para todo el tráfico entrante.
  - Si activa la conservación de la IP del cliente, los grupos de seguridad de las instancias deben permitir el tráfico procedente de los clientes. Además, las instancias deben estar en la misma VPC que el punto de conexión de EC2 Instance Connect.
  - Si desactiva la conservación de la IP del cliente, los grupos de seguridad de las instancias deben permitir el tráfico procedente de la VPC. Esta es la opción predeterminada.
  - Los siguientes tipos de instancia no admiten la preservación de IP de cliente: C1, CG1, CG2, G1, HI1, M1, M2, M3 y T1. Si activa la conservación de la IP del cliente e intenta conectarse a una instancia con uno de estos tipos de instancias mediante el punto de conexión de EC2 Instance Connect, se produce un error en la conexión.
  - No se admite la conservación de la IP del cliente cuando el tráfico se enruta a través de una puerta de enlace.
- Cuando crea un punto de conexión de EC2 Instance Connect, se crea automáticamente un rol vinculado a un servicio de Amazon EC2 en AWS Identity and Access Management (IAM). Amazon EC2 utiliza el rol vinculado a un servicio para aprovisionar las interfaces de red de su cuenta, que son necesarias para crear puntos de conexión de instancia de EC2 Instance Connect. Para obtener más información, consulte Rol vinculado a un servicio del punto de conexión de EC2 Instance Connect.
- Cada punto de conexión de EC2 Instance Connect puede admitir hasta 20 conexiones simultáneas.
- La duración máxima de una conexión TCP establecida es de 1 hora (3600 segundos). Puede especificar la duración máxima permitida en una política de IAM, que puede ser de 3600 segundos o menos. Para obtener más información, consulte Permisos para usar el punto de conexión de EC2 Instance Connect para conectarse a instancias.
- El punto de conexión de EC2 Instance Connect no se admite en el Oeste de Canadá (Calgary).

Concesión de permisos para el punto de conexión de EC2 Instance Connect

De forma predeterminada, las entidades de IAM no tienen permiso para crear, describir ni modificar puntos de conexión de EC2 Instance Connect. Un administrador de IAM puede crear políticas de IAM que concedan permisos necesarios para realizar acciones específicas en los recursos que necesitan.

Para obtener información acerca de las políticas de IAM, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

En los siguientes ejemplos de políticas, se muestra cómo puede controlar los permisos que tienen los usuarios para los puntos de conexión de EC2 Instance Connect.

Ejemplos

- Permisos para crear, describir y eliminar los puntos de conexión de EC2 Instance Connect
- Permisos para usar el punto de conexión de EC2 Instance Connect para conectarse a instancias
- Permisos para conectarse solo desde un rango de direcciones IP específico

Permisos para crear, describir y eliminar los puntos de conexión de EC2 Instance Connect

Para crear un punto de conexión de EC2 Instance Connect, es necesario que los usuarios tenga permisos para las siguientes acciones:

- `ec2:CreateInstanceConnectEndpoint`
- `ec2:CreateNetworkInterface`
- `ec2:CreateTags`
- `iam:CreateServiceLinkedRole`

Para describir y eliminar los puntos de conexión de EC2 Instance Connect, es necesario que los usuarios tengan permisos para las siguientes acciones:

- `ec2:DescribeInstanceConnectEndpoints`
- `ec2:DeleteInstanceConnectEndpoint`

Puede crear una política que conceda permisos para crear, describir y eliminar puntos de conexión de EC2 Instance Connect en todas las subredes. Como alternativa, puede restringir las acciones de subredes específicas. Solo hace falta especifiar los ARN de la subred como el `Resource` permitido o mediante la clave de condición `ec2:SubnetID`. También puede usar

la clave de condición `aws:ResourceTag` para permitir o denegar explícitamente la creación de puntos de conexión con determinadas etiquetas. Para obtener más información, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.

Política de IAM de ejemplo

En el siguiente ejemplo de política de IAM, la sección del `Resource` concede permiso para crear y eliminar puntos de conexión en todas las subredes, especificados con el asterisco (*). Las acciones de la API `ec2:Describe*` no admiten permisos de recursos. Por lo tanto, el carácter comodín * es necesario en el elemento `Resource`.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "GrantAllActionsInAllSubnets",
            "Action": [
                "ec2:CreateInstanceConnectEndpoint",
                "ec2:DeleteInstanceConnectEndpoint",
                "ec2:CreateNetworkInterface",
                "ec2:CreateTags",
                "iam:CreateServiceLinkedRole"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:ec2:region:account-id:subnet/*"
        },
        {
            "Action": [
                "ec2:CreateNetworkInterface"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:ec2:::security-group/*"
        },
        {
            "Sid": "DescribeInstanceConnectEndpoints",
            "Action": [
                "ec2:DescribeInstanceConnectEndpoints"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Permisos para usar el punto de conexión de EC2 Instance Connect para conectarse a instancias

La acción `ec2-instance-connect:OpenTunnel` concede permiso para establecer una conexión TCP a una instancia a fin de conectarse a través del punto de conexión de EC2 Instance Connect. Puede especificar el punto de conexión de EC2 Instance Connect que se va a utilizar. Como alternativa, un `Resource` con asterisco (`*`) permite a los usuarios utilizar cualquier punto de conexión de EC2 Instance Connect disponible. También puede restringir el acceso a las instancias en función de la presencia o ausencia de etiquetas de recursos como claves de condición.

Condiciones

- `ec2-instance-connect:remotePort`: el puerto de la instancia que se puede usar para establecer una conexión TCP. Cuando se utiliza esta clave de condición, se produce un error al intentar conectarse a una instancia en cualquier otro puerto que no sea el especificado en la política.
- `ec2-instance-connect:privateIpAddress`: la dirección IP privada de destino asociada a la instancia con la que se quiere establecer una conexión TCP. Puede especificar una sola dirección IP, por ejemplo `10.0.0.1/32`, o un rango de IP a través de los CIDR, como `10.0.1.0/28`. Cuando se usa esta clave de condición, se produce un error al intentar conectarse a una instancia con una dirección IP privada diferente o fuera del rango del CIDR.
- `ec2-instance-connect:maxTunnelDuration`: la duración máxima de una conexión TCP establecida. La unidad es segundos y la duración oscila entre un mínimo de 1 y un máximo de 3600 segundos (1 hora). Si no se especifica la condición, la duración predeterminada se establece en 3600 segundos (1 hora). Si intenta conectarse a una instancia durante más tiempo que el especificado en la política de IAM o durante más tiempo que el máximo predeterminado, se produce un error. La conexión termina una vez transcurrido el tiempo especificado.

  Si `maxTunnelDuration` se especifica en la política de IAM y su valor es inferior a 3600 segundos (el valor predeterminado), debe especificar `--max-tunnel-duration` en el comando al conectarse a una instancia. Para obtener más información sobre cómo conectarse a una instancia de base de datos, consulte Conexión a una instancia de Amazon EC2 mediante el punto de conexión de EC2 Instance Connect.

También puede conceder acceso a un usuario para establecer conexiones a las instancias en función de la presencia de etiquetas de recursos en el punto de conexión de EC2 Instance Connect. Para obtener más información, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.

Para instancias de Linux, la acción `ec2-instance-connect:SendSSHPublicKey` concede permiso a un usuario para insertar la clave pública en una instancia. La condición `ec2:osuser` especifica el nombre del usuario del SO (sistema operativo) que puede enviar la clave pública a una instancia. Utilice el nombre de usuario predeterminado para la AMI que se utilizó para lanzar la instancia. Para obtener más información, consulte Concesión de permisos de IAM para EC2 Instance Connect.

Política de IAM de ejemplo

Las siguientes políticas de IAM de ejemplo permiten que una entidad principal de IAM se conecte a una instancia con solo el punto de conexión de EC2 Instance Connect especificado, que se identifica por el ID de punto de conexión `eice-123456789abcdef` especificado. La conexión se establece correctamente solo si se cumplen todas las condiciones.

> **Note**
>
> Las acciones de la API `ec2:Describe*` no admiten permisos de recursos. Por lo tanto, el carácter comodín `*` es necesario en el elemento `Resource`.

Linux

En este ejemplo, se evalúa si la conexión a la instancia se establece en el puerto 22 (SSH), si la dirección IP privada de la instancia se encuentra dentro del intervalo de `10.0.1.0/31` (entre `10.0.1.0` y `10.0.1.1`) y `maxTunnelDuration` es inferior o igual a `3600` segundos. La conexión se pierde después de `3600` segundos (1 hora).

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "EC2InstanceConnect",
            "Action": "ec2-instance-connect:OpenTunnel",
            "Effect": "Allow",
            "Resource": "arn:aws:ec2:region:account-id:instance-connect-
endpoint/eice-123456789abcdef",
            "Condition": {
                "NumericEquals": {
                    "ec2-instance-connect:remotePort": "22"
                },
                "IpAddress": {
```

```
                    "ec2-instance-connect:privateIpAddress": "10.0.1.0/31"
                },
                "NumericLessThanEquals": {
                    "ec2-instance-connect:maxTunnelDuration": "3600"
                }
            }
        },
        {
            "Sid": "SSHPublicKey",
            "Effect": "Allow",
            "Action": "ec2-instance-connect:SendSSHPublicKey",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:osuser": "ami-username"
                }
            }
        },
        {
            "Sid": "Describe",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceConnectEndpoints"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Windows

En este ejemplo, se evalúa si la conexión a la instancia se establece en el puerto 3389 (RDP), si la dirección IP privada de la instancia se encuentra dentro del intervalo de `10.0.1.0/31` (entre `10.0.1.0` y `10.0.1.1`) y `maxTunnelDuration` es inferior o igual a `3600` segundos. La conexión se pierde después de `3600` segundos (1 hora).

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "EC2InstanceConnect",
            "Action": "ec2-instance-connect:OpenTunnel",
            "Effect": "Allow",
```

```
            "Resource": "arn:aws:ec2:region:account-id:instance-connect-
endpoint/eice-123456789abcdef",
            "Condition": {
                "NumericEquals": {
                    "ec2-instance-connect:remotePort": "3389"
                },
                "IpAddress": {
                    "ec2-instance-connect:privateIpAddress": "10.0.1.0/31"
                },
                "NumericLessThanEquals": {
                    "ec2-instance-connect:maxTunnelDuration": "3600"
                }
            }
        },
        {
            "Sid": "Describe",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceConnectEndpoints"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Permisos para conectarse solo desde un rango de direcciones IP específico

El siguiente ejemplo de política de IAM permite que una entidad principal de IAM se conecte a una instancia con la condición de que lo haga desde una dirección IP dentro del rango de direcciones IP especificado en la política. Si la entidad principal de IAM llama a `OpenTunnel` desde una dirección IP que no esté dentro de `192.0.2.0/24` (el rango de direcciones IP de ejemplo de esta política), la respuesta será `Access Denied`. Para obtener más información, consulte `aws:SourceIp` en la Guía del usuario de IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": "ec2-instance-connect:OpenTunnel",
            "Resource": "arn:aws:ec2:region:account-id:instance-connect-
endpoint/eice-123456789abcdef",
```

```
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": "192.0.2.0/24"
                },
                "NumericEquals": {
                    "ec2-instance-connect:remotePort": "22"
                }
            }
        },
        {
            "Sid": "SSHPublicKey",
            "Effect": "Allow",
            "Action": "ec2-instance-connect:SendSSHPublicKey",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:osuser": "ami-username"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceConnectEndpoints"
            ],
            "Resource": "*"
        }
    ]
}
```

Grupos de seguridad para el punto de conexión de EC2 Instance Connect

Un grupo de seguridad controla el tráfico al que se permite llegar y dejar los recursos a los que está asociado. Por ejemplo, denegamos el tráfico hacia y desde una instancia de Amazon EC2 a menos que los grupos de seguridad asociados a la instancia lo permitan específicamente.

En los siguientes ejemplos, se muestra cómo configurar las reglas del grupo de seguridad para el punto de conexión de EC2 Instance Connect y las instancias de destino.

Ejemplos

- Reglas del grupo de seguridad del punto de conexión de EC2 Instance Connect

- Reglas del grupo de seguridad de instancias de destino

Reglas del grupo de seguridad del punto de conexión de EC2 Instance Connect

Las reglas del grupo de seguridad de un punto de conexión de EC2 Instance Connect deben permitir el tráfico saliente para que las instancias de destino abandonen el punto de conexión. Puede especificar el grupo de seguridad de la instancia o el rango de direcciones IPv4 de la VPC como destino.

El tráfico al punto de conexión se origina en el servicio del punto de conexión de EC2 Instance Connect y se permite independientemente de las reglas de entrada del grupo de seguridad del punto de conexión. Para controlar quién puede usar el punto de conexión de EC2 Instance Connect para conectarse a una instancia, utilice una política de IAM. Para obtener más información, consulte Permisos para usar el punto de conexión de EC2 Instance Connect para conectarse a instancias.

Ejemplo de regla de salida: referencia a grupos de seguridad

En el siguiente ejemplo, se utiliza la referencia a grupos de seguridad, lo que significa que el destino es un grupo de seguridad asociado a las instancias de destino. Esta regla permite el tráfico saliente desde el punto de conexión a todas las instancias que utilizan este grupo de seguridad.

Protocolo	Destino	Intervalo de puertos	Comentario
TCP	*ID del grupo de seguridad de la instancia*	22	Permite el tráfico SSH saliente a todas las instancias asociadas al grupo de seguridad de la instancia

Ejemplo de regla de salida: rango de direcciones IPv4

En el siguiente ejemplo, se permite el tráfico saliente al rango de direcciones IPv4 especificado. Las direcciones IPv4 de una instancia se asignan desde su subred, por lo que puede usar el rango de direcciones IPv4 de la VPC.

Protocolo	Destino	Intervalo de puertos	Comentario
TCP	*CIDR IPv4 de VPC*	22	Permite el tráfico SSH saliente a la VPC

Reglas del grupo de seguridad de instancias de destino

Las reglas del grupo de seguridad para instancias de destino deben permitir el tráfico entrante desde el punto de conexión de EC2 Instance Connect. Puede especificar el grupo de seguridad del punto de conexión o un rango de direcciones IPv4 como el origen. Si especifica un rango de direcciones IPv4, el origen depende de si la conservación de la IP del cliente está desactivada o activada. Para obtener más información, consulte Consideraciones.

Como los grupos de seguridad tienen estado, se permite que el tráfico de respuesta abandone la VPC independientemente de las reglas de salida del grupo de seguridad de la instancia.

Ejemplo de regla de entrada: referencia a grupos de seguridad

En el siguiente ejemplo, se utiliza la referencia a grupos de seguridad, lo que significa que el origen es un grupo de seguridad asociado al punto de conexión. Esta regla permite el tráfico SSH entrante desde el punto de conexión a todas las instancias que utilizan este grupo de seguridad, independientemente de que la conservación de la IP del cliente esté activada o desactivada. Si no hay otras reglas de grupos de seguridad entrantes para SSH, las instancias solo aceptan el tráfico SSH desde el punto de conexión.

Protocolo	Origen	Intervalo de puertos	Comentario
TCP	*ID del grupo de seguridad del punto de conexión*	22	Permite el tráfico SSH entrante desde los recursos asociados al grupo de seguridad del punto de conexión

Ejemplo de regla de entrada: conservación de la IP del cliente desactivada

En el siguiente ejemplo, se permite el tráfico SSH entrante procedente del rango de direcciones IPv4 especificado. Como la conservación de la IP del cliente está desactivada, la dirección IPv4 de origen es la dirección de la interfaz de red del punto de conexión. La dirección de la interfaz de red del punto de conexión se asigna desde su subred, por lo que puede usar el rango de direcciones IPv4 de la VPC para permitir las conexiones a todas las instancias de la VPC.

Protocolo	Origen	Intervalo de puertos	Comentario
TCP	*CIDR IPv4 de VPC*	22	Se permite el tráfico SSH entrante procedente de la VPC

Ejemplo de regla de entrada: conservación de la IP del cliente activada

En el siguiente ejemplo, se permite el tráfico SSH entrante procedente del rango de direcciones IPv4 especificado. Como la conservación de la IP del cliente está activada, la dirección IPv4 de origen es la dirección del cliente.

Protocolo	Origen	Intervalo de puertos	Comentario
TCP	*Rango de direcciones IPv4 públicas*	22	Se permite el tráfico entrante procedente del rango de direcciones IPv4 del cliente especificado

Creación de un punto de conexión de EC2 Instance Connect

Puede crear un punto de conexión de EC2 Instance Connect para permitir una conexión segura a las instancias.

No puede modificar un punto de conexión de EC2 Instance Connect después de haberlo creado. En su lugar, debe eliminar el punto de conexión de EC2 Instance Connect y crear uno nuevo con la configuración que necesite.

Requisitos previos

Debe tener los permisos de IAM necesarios para crear un punto de conexión de EC2 Instance Connect. Para obtener más información, consulte Permisos para crear, describir y eliminar los puntos de conexión de EC2 Instance Connect.

Subredes compartidas

Puede crear un punto de conexión de EC2 Instance Connect en una subred que le han compartido. No puede utilizar un punto de conexión de EC2 Instance Connect creado por el propietario de la VPC en una subred que le han compartido.

Crear un punto de conexión usando la consola

Utilice uno de los siguientes métodos para crear un punto de conexión de EC2 Instance Connect.

Para crear un punto de conexión de EC2 Instance Connect

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación izquierdo, seleccione Puntos de conexión.
3. Elija Crear punto de conexión y, a continuación, especifique la configuración del punto de conexión de la siguiente manera:
   a. (Opcional) En Etiqueta de nombre, ingrese un nombre para el punto de conexión.
   b. En Categoría de servicio, elija Punto de conexión de EC2 Instance Connect.
   c. En VPC, elija la VPC que contiene las instancias de destino.
   d. (Opcional) Para conservar las direcciones IP de los clientes, expanda Configuración adicional y active la casilla de verificación. De lo contrario, el valor predeterminado es utilizar la interfaz de red del punto de conexión como dirección IP del cliente.
   e. (Opcional) En Grupos de seguridad, seleccione el grupo de seguridad que quiera asociar al punto de conexión. De lo contrario, se usará el grupo de seguridad predeterminado para la VPC. Para obtener más información, consulte Grupos de seguridad para el punto de conexión de EC2 Instance Connect.
   f. En Subredes, seleccione la subred en la cual crear el punto de conexión.
   g. (Opcional) Para agregar una etiqueta, elija Agregar etiqueta nueva e ingrese la clave y el valor de la etiqueta.
4. Revise la configuración y, a continuación, seleccione Crear punto de conexión.

El estado inicial del punto de conexión es Pendiente. Antes de poder conectarse a una instancia mediante este punto de conexión, debe esperar hasta que el estado del punto de conexión sea Disponible. Este proceso puede tardar unos minutos.

5. Si quiere utilizar el punto de conexión para conectarse a una instancia, consulte Conexión a una instancia.

Crear un punto de conexión con la AWS CLI

Utilice el comando de la AWS CLI create-instance-connect-endpoint:

Requisitos previos

Instale la versión 2 de la AWS CLI y configúrela con sus credenciales. Para obtener más información, consulte Instalación o actualización de la versión más reciente de AWS CLI y Configuración de AWS CLI en la Guía del usuario de AWS Command Line Interface. Como alternativa, abra AWS CloudShell y ejecute los comandos de AWS CLI en el intérprete de comandos previamente autenticado.

Para crear el punto de enlace

Utilice el siguiente comando para crear una interfaz de red de puntos de conexión para su punto de conexión de EC2 Instance Connect en la subred especificada.

```
aws ec2 create-instance-connect-endpoint --subnet-id subnet-0123456789example
```

A continuación, se muestra un ejemplo del resultado.

```
 {
        "OwnerId": "111111111111",
        "InstanceConnectEndpointId": "eice-0123456789example",
        "InstanceConnectEndpointArn": "arn:aws:ec2:us-east-1:111111111111:instance-
connect-endpoint/eice-0123456789example",
        "State": "create-complete",
        "StateMessage": "",
        "DnsName": "eice-0123456789example.0123abcd.ec2-instance-connect-endpoint.us-
east-1.amazonaws.com",
        "FipsDnsName": "eice-0123456789example.0123abcd.fips.ec2-instance-connect-
endpoint.us-east-1.amazonaws.com",
        "NetworkInterfaceIds": [
```

```
            "eni-0123abcd"
        ],
        "VpcId": "vpc-0123abcd",
        "AvailabilityZone": "us-east-1a",
        "CreatedAt": "2023-04-07T15:43:53.000Z"
        "SubnetId": "subnet-0123abcd",
        "PreserveClientIp": false,
        "SecurityGroupIds": [
            "sg-0123abcd"
        ],
        "Tags": []
}
```

Para supervisar el estado de creación

El valor inicial para el campo `State` es `create-in-progress`. Antes de poder conectarse a una instancia mediante este punto de conexión, espere hasta que el estado sea `create-complete`. Utilice el comando describe-instance-connect-endpoints de la AWS CLI para supervisar el estado del punto de conexión de EC2 Instance Connect. El parámetro --query filtra los resultados y los envía al campo `State`.

```
aws ec2 describe-instance-connect-endpoints --instance-connect-endpoint-
ids eice-0123456789example --query InstanceConnectEndpoints[*].State --output text
```

A continuación, se muestra un ejemplo del resultado.

```
create-complete
```

Conexión a una instancia de Amazon EC2 mediante el punto de conexión de EC2 Instance Connect

Puede usar el punto de conexión de EC2 Instance Connect para conectarse a una instancia de Amazon EC2 que admita SSH o RDP.

Contenido

Requisitos previos

- Debe tener el permiso de IAM necesario para conectarse a un punto de conexión de EC2 Instance Connect. Para obtener más información, consulte Permisos para usar el punto de conexión de EC2 Instance Connect para conectarse a instancias.
- El punto de conexión de EC2 Instance Connect debe estar en el estado Disponible (consola) o `create-complete` (AWS CLI). Si no tiene un punto de conexión de EC2 Instance Connect para su VPC, puede crear uno. Para obtener más información, consulte Creación de un punto de conexión de EC2 Instance Connect.
- (Instancias de Linux) Para utilizar la consola de EC2 para conectarse a la instancia, o para utilizar la CLI para conectarse y hacer que EC2 Instance Connect gestione la clave efímera, la instancia debe tener instalado EC2 Instance Connect. Para obtener más información, consulte Instalación de EC2 Instance Connect.
- Asegúrese de que el grupo de seguridad de la instancia permita el tráfico SSH entrante desde el punto de conexión de EC2 Instance Connect. Para obtener más información, consulte Reglas del grupo de seguridad de instancias de destino.

Conexión a la instancia de Linux con la consola de Amazon EC2

Puede conectarse a una instancia mediante la consola de Amazon EC2 de la siguiente manera.

Para conectarse a la instancia mediante el cliente basado en navegador

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Seleccione la instancia y elija Connect.
4. Elija la pestaña EC2 Instance Connect.
5. En Tipo de conexión, elija Conectarse a una instancia mediante el punto de conexión de EC2 Instance Connect.
6. En Punto de conexión de EC2 Instance Connect, elija el ID del punto de conexión de EC2 Instance Connect.
7. En el caso del nombre de usuario, si la AMI que utilizó para iniciar la instancia utiliza un nombre de usuario que no sea `ec2-user`, introduzca el nombre de usuario correcto.
8. En Duración máxima del túnel (segundos), ingrese la duración máxima permitida de la conexión SSH.

La duración debe cumplir con la condición `maxTunnelDuration` especificada en la política de IAM. Si no se tiene acceso a la política de IAM, contáctese con su administrador.

9. Elija Conectar. Esto abre una ventana de terminal para la instancia.

Conectarse a la instancia de Linux con SSH

Puede usar SSH para conectarse a la instancia de Linux y usar el comando `open-tunnel` para establecer un túnel privado. Se puede utilizar `open-tunnel` en los modos de conexión única o múltiple.

Para obtener más información acerca del uso de la AWS CLI para conectarse a la instancia de mediante SSH, consulte Conexión mediante la AWS CLI.

El siguiente ejemplo usa OpenSSH. Puede usar cualquier otro cliente SSH que admita el modo proxy.

Conexión única de

Para permitir solo una conexión a una instancia mediante SSH y el comando **`open-tunnel`**

Utilice `ssh` y el comando de AWS CLI open-tunnel de la siguiente manera: El comando de proxy `-o` incluye el comando `open-tunnel` que crea el túnel privado hacia la instancia.

```
ssh -i my-key-pair.pem ec2-user@i-0123456789example \
    -o ProxyCommand='aws ec2-instance-connect open-tunnel --instance-
id i-0123456789example'
```

Para:

- `-i`: especifique el par de claves que se usó para iniciar la instancia.
- *`ec2-user`*`@`*`i-0123456789example`*: especifique el nombre de usuario de la AMI que se usó para iniciar la instancia y el ID de la instancia.
- `--instance-id`: especifique el ID de la instancia a la que se va a conectar. Como alternativa, especifique `%h`, que extrae el ID de instancia del usuario.

Conexión múltiple

Para permitir varias conexiones a una instancia, primero ejecute el comando de AWS CLI open-tunnel para iniciar la escucha de nuevas conexiones TCP y, a continuación, use `ssh` para crear una nueva conexión TCP y un túnel privado hacia la instancia.

Para permitir varias conexiones a la instancia mediante SSH y el comando **`open-tunnel`**

1. Ejecute el siguiente comando para iniciar la escucha de nuevas conexiones TCP en el puerto especificado del equipo local.

   ```
   aws ec2-instance-connect open-tunnel \
       --instance-id i-0123456789example \
       --local-port 8888
   ```

   Resultado previsto

   ```
   Listening for connections on port 8888.
   ```

2. En una nueva ventana de terminal, ejecute el comando `ssh` para crear una nueva conexión TCP y un túnel privado para la instancia.

   ```
   ssh -i my-key-pair.pem ec2-user@localhost -p 8888
   ```

   Salida esperada: en la primera ventana de terminal, aparecerá lo siguiente:

   ```
   [1] Accepted new tcp connection, opening websocket tunnel.
   ```

   Es posible que vea el siguiente código de error:

   ```
   [1] Closing tcp connection.
   ```

Conexión a la instancia de Linux con la AWS CLI

Si conoce solo el ID de la instancia, puede utilizar el comando ec2-instance-connect AWS CLI para conectarse a ella mediante un cliente SSH. Para obtener más información sobre el uso del comando ec2-instance-connect, consulte Conexión mediante la AWS CLI.

Requisitos previos

Instale la versión 2 de la AWS CLI y configúrela con sus credenciales. Para obtener más información, consulte Instalación o actualización de la versión más reciente de AWS CLI y Configuración de AWS CLI en la Guía del usuario de AWS Command Line Interface. Como alternativa, abra AWS CloudShell y ejecute los comandos de AWS CLI en el intérprete de comandos previamente autenticado.

Para conectarse a una instancia mediante el ID de instancia y un punto de conexión de EC2 Instance Connect

Si solo conoce el ID de la instancia, utilice el comando de CLI ec2-instance-connect y especifique el comando `ssh`, el ID de la instancia y el parámetro `--connection-type` con el valor `eice`.

```
aws ec2-instance-connect ssh --instance-id i-1234567890example --connection-type eice
```

> **Tip**
>
> Si aparece un error al usar este comando, asegúrese de que usa la AWS CLI versión 2. El parámetro `ssh` solo está disponible para la AWS CLI versión 2. Para obtener más información, consulte Información AWS CLI sobre la versión 2 en la AWS Command Line InterfaceGuía del usuario.

Conexión a la instancia de Windows mediante el punto de conexión de EC2 Instance Connect

Puede usar el protocolo de escritorio remoto (RDP) a través del punto de conexión de EC2 Instance Connect para conectarse a una instancia de Windows sin una dirección IPv4 pública ni un nombre de DNS público.

Para conectarse a la instancia de Windows mediante un cliente RDP

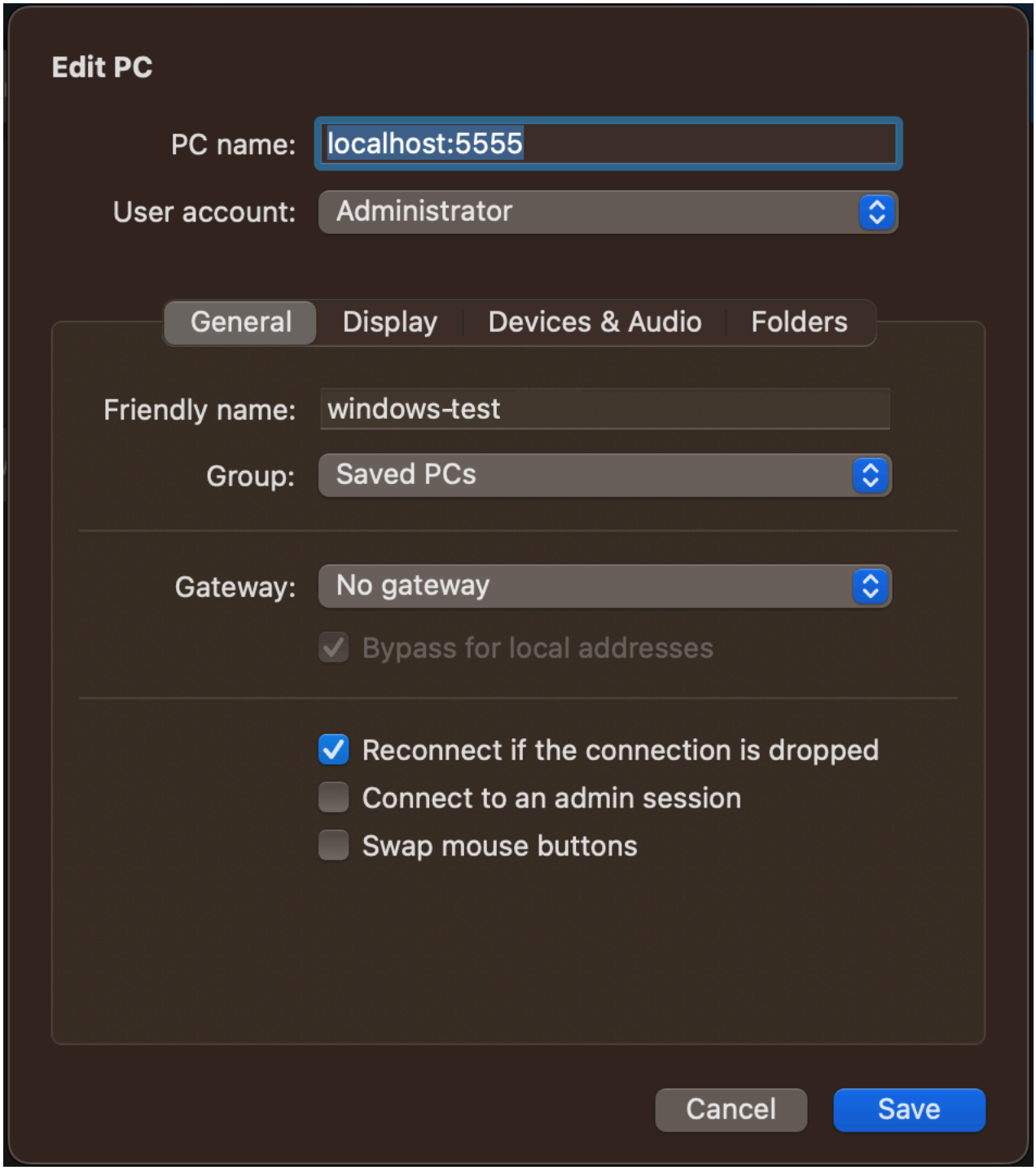
1. Complete los pasos del 1 al 8 en Conectarse a una instancia de Windows mediante RDP. Tras descargar el archivo de escritorio de RDP en el paso 8, aparecerá el mensaje No se puede conectar, lo cual es de esperar porque la instancia no tiene una dirección IP pública.
2. Ejecute el siguiente comando para establecer un túnel privado hacia la VPC en la que se encuentra la instancia. `--remote-port` debe tener el valor `3389` porque RDP usa el puerto 3389 de forma predeterminada.

   ```
   aws ec2-instance-connect open-tunnel \
   ```

```
    --instance-id i-0123456789example \
    --remote-port 3389 \
    --local-port any-port
```

3. En la carpeta Descargas, busque el archivo de escritorio de RDP que descargó y arrástrelo a la ventana del cliente de RDP.
4. Haga clic con el botón derecho en el archivo de escritorio de RDP y elija Editar.
5. En la ventana Editar PC, ingrese `localhost:local-port` en Nombre del PC (la instancia a la que conectarse), donde *`local-port`* utilizará el mismo valor que en el paso 2 y, a continuación, seleccione Guardar.

   Tenga en cuenta que la siguiente captura de pantalla de la ventana Editar PC procede de Escritorio remoto de Microsoft en un Mac. Si utiliza un cliente Windows, la ventana puede ser diferente.



6. En el cliente RDP, haga clic con el botón derecho en el PC (que acaba de configurar) y elija Conectar para conectarse a su instancia.
7. En la solicitud, ingrese la contraseña descifrada de la cuenta de administrador.

Solución de problemas

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que pueda encontrar al utilizar el punto de conexión de EC2 Instance Connect para conectar una instancia.

No puede conectarse a su instancia

Los siguientes son los motivos habituales por los que es posible que no pueda conectarse a su instancia.

- Grupos de seguridad: compruebe los grupos de seguridad asignados al punto de conexión de EC2 Instance Connect y su instancia. Para obtener más información acerca de las reglas de los grupos de seguridad obligatorios, consulte Grupos de seguridad para el punto de conexión de EC2 Instance Connect.
- Estado de instancia: compruebe que la instancia esté en el estado `running`.
- Par de claves: si el comando que usa para conectarse requiere una clave privada, compruebe que la instancia tenga una clave pública y que dispone de la clave privada correspondiente.
- Permisos de IAM: compruebe que dispone de los permisos de IAM necesarios. Para obtener más información, consulte Concesión de permisos para el punto de conexión de EC2 Instance Connect.

Para obtener más consejos de solución de problemas para instancias de Linux, consulte Solución de problemas de conexión a la instancia de Linux. Para obtener más consejos de solución de problemas para instancias de Windows, consulte the section called “Conexión con la instancia de Windows de”.

ErrorCode: AccessDeniedException

Si aparece un error `AccessDeniedException` y la condición `maxTunnelDuration` se especifica en la política de IAM, asegúrese de especificar el parámetro `--max-tunnel-duration` al conectarse a una instancia. Para obtener más información sobre este parámetro, consulte open-tunnel en la Referencia de comandos de AWS CLI.

Registro de las conexiones establecidas en el punto de conexión de EC2 Instance Connect

Puede registrar las operaciones de los recursos y auditar las conexiones establecidas en el punto de conexión de EC2 Instance Connect con los registros de AWS CloudTrail.

Para obtener más información sobre el uso de AWS CloudTrail con Amazon EC2, consulte Registro de llamadas a la API de Amazon EC2 mediante AWS CloudTrail.

Registro de las llamadas a la API del punto de conexión de EC2 Instance Connect con AWS CloudTrail

Las operaciones de recursos del punto de conexión de EC2 Instance Connect se registran en CloudTrail como eventos de administración. Cuando se hacen las siguientes llamadas a la API, la actividad se registra como un evento de CloudTrail en Historial de eventos:

- `CreateInstanceConnectEndpoint`
- `DescribeInstanceConnectEndpoints`
- `DeleteInstanceConnectEndpoint`

Puede ver, buscar y descargar los últimos eventos en su Cuenta de AWS. Para obtener más información, consulte Visualización de eventos con el historial de eventos de CloudTrail en la Guía del usuario de AWS CloudTrail.

AWS CloudTrail se utiliza para auditar a los usuarios que se conectan a una instancia mediante el punto de conexión de EC2 Instance Connect

Los intentos de conexión a instancias a través del punto de conexión de EC2 Instance Connect se registran en CloudTrail en el historial de eventos. Cuando se inicia una conexión a una instancia a través de un punto de conexión de EC2 Instance Connect, la conexión se registra como un evento de administración de CloudTrail con el `eventName` de `OpenTunnel`.

Puede crear reglas de Amazon EventBridge que enruten el evento de CloudTrail a un destino. Para más información, consulte la Guía del usuario de Amazon EventBridge.

A continuación se muestra un ejemplo de un evento de administración `OpenTunnel` que se registró en CloudTrail.

```
{
     "eventVersion": "1.08",
     "userIdentity": {
         "type": "IAMUser",
         "principalId": "ABCDEFGONGNOMOOCB6XYTQEXAMPLE",
         "arn": "arn:aws:iam::1234567890120:user/IAM-friendly-name",
         "accountId": "123456789012",
         "accessKeyId": "ABCDEFGUKZHNAW4OSN2AEXAMPLE",
         "userName": "IAM-friendly-name"
     },
     "eventTime": "2023-04-11T23:50:40Z",
```

```
    "eventSource": "ec2-instance-connect.amazonaws.com",
    "eventName": "OpenTunnel",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "1.2.3.4",
    "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
    "requestParameters": {
        "instanceConnectEndpointId": "eici-0123456789EXAMPLE",
        "maxTunnelDuration": "3600",
        "remotePort": "22",
        "privateIpAddress": "10.0.1.1"
    },
    "responseElements": null,
    "requestID": "98deb2c6-3b3a-437c-a680-03c4207b6650",
    "eventID": "bbba272c-8777-43ad-91f6-c4ab1c7f96fd",
    "readOnly": false,
    "resources": [{
        "accountId": "123456789012",
        "type": "AWS::EC2::InstanceConnectEndpoint",
        "ARN": "arn:aws:ec2:us-east-1:123456789012:instance-connect-endpoint/
eici-0123456789EXAMPLE"
    }],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

Eliminar un punto de conexión de EC2 Instance Connect

Cuando ya no necesite un punto de conexión de EC2 Instance Connect, puede eliminarlo.

Debe tener los permisos de IAM necesarios para crear un punto de conexión de EC2 Instance Connect. Para obtener más información, consulte Permisos para crear, describir y eliminar los puntos de conexión de EC2 Instance Connect.

Al eliminar un punto de conexión de EC2 Instance Connect con la consola, primero pasa al estado Eliminando. Si la eliminación se realiza correctamente, el punto de conexión eliminado ya no aparece. Si se produce un error en la eliminación, el estado es `delete-failed` y el Mensaje de estado indica el motivo del error.

Al eliminar un punto de conexión de EC2 Instance Connect mediante la AWS CLI, pasa al estado `delete-in-progress`. Si la eliminación se realiza correctamente, pasa al estado `delete-`

`complete`. Si se produce un error en la eliminación, el estado es `delete-failed` y el motivo del error se indica en el `StateMessage`.

Console

Para eliminar un punto de conexión de EC2 Instance Connect

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación izquierdo, seleccione Puntos de conexión.
3. Selección del punto de conexión.
4. Elija Acciones, Eliminar puntos de conexión de VPC.
5. Cuando se le solicite confirmación, ingrese **`delete`**.
6. Elija Delete (Eliminar).

AWS CLI

Para eliminar un punto de conexión de EC2 Instance Connect

Utilice el comando de AWS CLI delete-instance-connect-endpoints y especifique el ID del punto de conexión de EC2 Instance Connect que se debe eliminar.

```
aws ec2 delete-instance-connect-endpoint --instance-connect-endpoint-
id eice-03f5e49b83924bbc7
```

Ejemplo de resultado

```
{
    "InstanceConnectEndpoint": {
        "OwnerId": "111111111111",
        "InstanceConnectEndpointId": "eice-0123456789example",
        "InstanceConnectEndpointArn": "arn:aws:ec2:us-east-1:111111111111:instance-
connect-endpoint/eice-0123456789example",
        "State": "delete-in-progress",
        "StateMessage": "",
        "NetworkInterfaceIds": [],
        "VpcId": "vpc-0123abcd",
        "AvailabilityZone": "us-east-1d",
        "CreatedAt": "2023-02-07T12:05:37+00:00",
        "SubnetId": "subnet-0123abcd"
```

```
    }
}
```

Rol vinculado a un servicio del punto de conexión de EC2 Instance Connect

Amazon EC2 utiliza roles vinculados a servicios de AWS Identity and Access Management (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM que se encuentra vinculado directamente a Amazon ECS. Los roles vinculados a servicios están predefinidos por Amazon EC2 e incluyen todos los permisos que Amazon EC2 necesita para llamar a otros Servicios de AWS en su nombre. Para obtener más información, consulte Uso de roles vinculados a servicios en la Guía del usuario de IAM.

Permisos de roles vinculados a un servicio del punto de conexión de EC2 Instance Connect

Amazon EC2 usa AWSServiceRoleForEC2InstanceConnect para crear y administrar las interfaces de red de la cuenta que requiere el punto de conexión de EC2 Instance Connect.

El rol vinculado a un servicio AWSServiceRoleForEC2InstanceConnect confía en que los siguientes servicios asuman el rol:

- `ec2-instance-connect.amazonaws.com`

El rol vinculado a un servicio AWSServiceRoleForEC2InstanceConnect utiliza la política administrada Ec2InstanceConnectEndpoint. Para ver los permisos de esta política, consulte Ec2InstanceConnectEndpoint en la Referencia de políticas administradas de AWS.

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Creación del rol vinculado a un servicio para el punto de conexión de EC2 Instance Connect

No necesita crear manualmente el rol vinculado a servicios. Cuando crea un punto de conexión de EC2 Instance Connect, Amazon EC2 crea el rol vinculado al servicio para usted.

Edición del rol vinculado a un servicio del punto de conexión de EC2 Instance Connect

El punto de conexión de EC2 Instance Connect no permite editar el rol vinculado a un servicio AWSServiceRoleForEC2InstanceConnect.

Eliminación del rol vinculado a un servicio del punto de conexión de EC2 Instance Connect

Si ya no tiene que utilizar el punto de conexión de EC2 Instance Connect, le recomendamos que elimine el rol vinculado a un servicio AWSServiceRoleForEC2InstanceConnect.

Puede eliminar el rol vinculado a un servicio solo después de eliminar todos los recursos del punto de conexión de EC2 Instance Connect.

Para obtener información sobre la eliminación de roles vinculados a servicios, consulte Eliminar un rol vinculado a un servicio en la Guía del usuario de IAM.

Cupo del Punto de conexión de EC2 Instance Connect

Su Cuenta de AWS tiene cuotas predeterminadas, anteriormente conocidas como “límites”, para cada servicio de AWS. A menos que se indique lo contrario, cada cuota es específica de la región de .

Su Cuenta de AWS tiene los siguientes cupos en relación con los puntos de conexión de EC2 Instance Connect.

Descripción	Cuota
Número máximo de puntos de conexión de EC2 Instance Connect por Cuenta de AWS por Región de AWS	5
Número máximo de puntos de conexión de EC2 Instance Connect por VPC	1
Número máximo de puntos de conexión de EC2 Instance Connect por subred	1
Número máximo de conexiones simultáneas por punto de conexión de EC2 Instance Connect	20

Conexión de una instancia de EC2 a un recurso de AWS

Después de iniciar una instancia, puede conectarla a uno o varios recursos de AWS.

Esta sección describe cómo conectar automáticamente una instancia de Amazon EC2 a una base de datos de Amazon RDS.

Conexión automática de una instancia de EC2 a una base de datos de RDS

Puede utilizar la característica de conexión automática de la consola de Amazon EC2 para conectar rápidamente una o más instancias de EC2 a una base de datos de RDS y permitir el tráfico entre ellas.

Para obtener más información, consulte Cómo se configura automáticamente la conexión. Para obtener una guía detallada, lo que incluye otras formas de conectar una instancia de EC2 y una base de datos de RDS, consulte Tutorial: conexión de una instancia de Amazon EC2 a una base de datos de Amazon RDS.

Temas

Costos

Si bien la conexión automática de una instancia de EC2 a una base de datos de RDS es gratuita, se le cobrarán los servicios subyacentes. Se aplicarán tarifas de transferencia de datos si la instancia de EC2 y la base de datos de RDS se encuentran en distintas zonas de disponibilidad. Para obtener más información sobre las tarifas de transferencia de datos, consulte la sección Transferencia de datos en la página Precios de las instancias bajo demanda de Amazon EC2.

Requisitos previos

Antes de poder conectar automáticamente una instancia de EC2 a una base de datos de RDS, compruebe lo siguiente:

- Las instancias de EC2 deben tener el estado Running (En ejecución). No puede conectar una instancia de EC2 si se encuentra en otro estado.
- Las instancias de EC2 y la base de datos de RDS deben estar en la misma nube privada virtual (VPC). La característica de conexión automática no se admite si una instancia de EC2 y una base de datos de RDS están en distintas VPC.

Conexión automática de una instancia y una base de datos

Puede conectar automáticamente una instancia de EC2 a una base de datos de RDS inmediatamente después de iniciar la instancia o más adelante.

Conexión automática inmediatamente después de la inicialización

Siga los pasos que se indican a continuación para conectar automáticamente una instancia de EC2 a una base de datos de RDS inmediatamente después de iniciar la instancia de EC2.

Para ver una animación de estos pasos, consulte Ver animación: conexión automática de una instancia de EC2 recién iniciada a una base de datos de RDS.

Para conectar automáticamente una instancia de EC2 recién iniciada a una base de datos de RDS mediante la consola de EC2

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de la consola, elija Launch instance (iniciar instancias) y, a continuación, siga los pasos para iniciar una instancia.
3. En la página de confirmación de la inicialización de la instancia, elija Connect an RDS database (Conectar una base de datos de RDS).
4. En el cuadro de diálogo Connect RDS Database (Conectar la base de datos de RDS), haga lo siguiente:

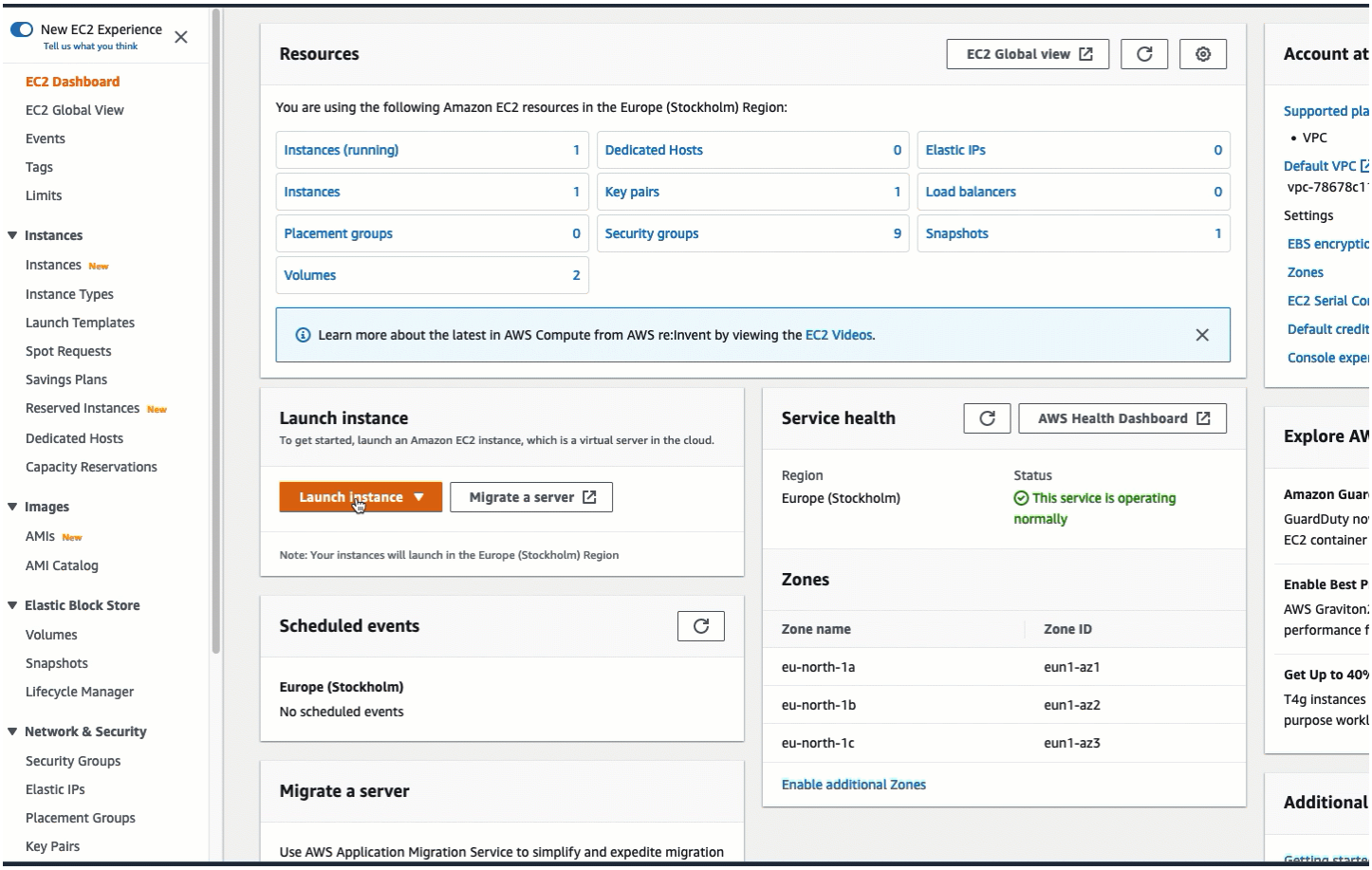
   a. En Database role (Rol de base de datos), elija Cluster (Clúster) o Instance (instancia).

   b. En RDS database (Base de datos de RDS), seleccione una base de datos a la que conectarse.

   > **Note**
   >
   > Las instancias de EC2 y la base de datos de RDS deben estar en la misma VPC para poder conectarse entre sí.

   c. Elija Conectar.

Ver animación: conexión automática de una instancia de EC2 recién iniciada a una base de datos de RDS



Conexión automática de una instancia existente

Siga los pasos que se indican a continuación para conectar automáticamente una instancia de EC2 existente a una base de datos de RDS.

Para ver una animación de estos pasos, consulte Ver animación: conexión automática de una instancia de EC2 a una base de datos de RDS.

Para conectar automáticamente una instancia de EC2 existente a una base de datos de RDS mediante la consola de EC2

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Seleccione una o más instancias de EC2 para conectarlas a una base de datos de RDS y, a continuación, elija Actions (Acciones), Networking (Redes), Connect RDS database (Conectar la base de datos de RDS).

Si Conectar la base de datos de RDS no está disponible, compruebe que el estado de las instancias de EC2 sea En ejecución y que estén en la misma VPC.

4. En el cuadro de diálogo Connect RDS Database (Conectar la base de datos de RDS), haga lo siguiente:

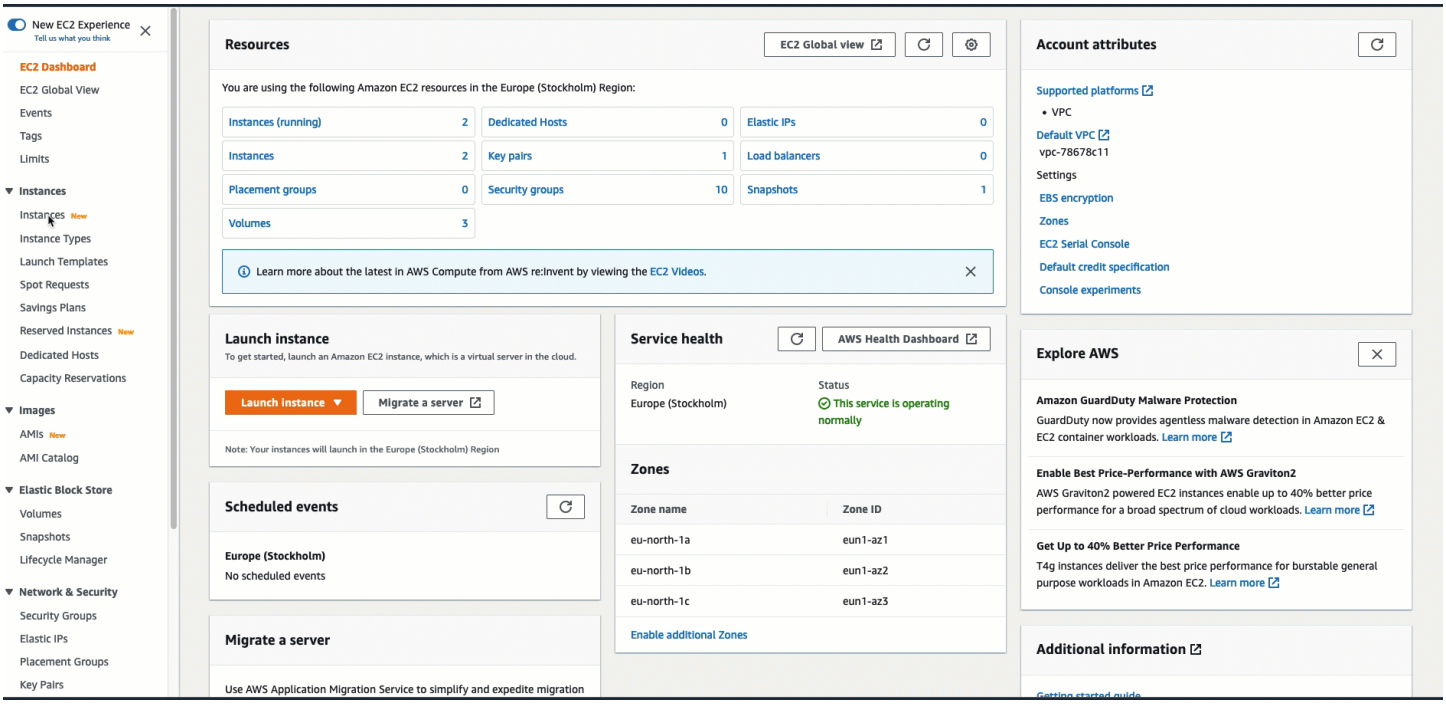
   a. En Database role (Rol de base de datos), elija Cluster (Clúster) o Instance (instancia).

   b. En RDS database (Base de datos de RDS), seleccione una base de datos a la que conectarse.

   > **Note**
   >
   > Las instancias de EC2 y la base de datos de RDS deben estar en la misma VPC para poder conectarse entre sí.

   c. Elija Conectar.

Ver animación: conexión automática de una instancia de EC2 a una base de datos de RDS



Para obtener información sobre cómo usar la consola de Amazon RDS para conectar automáticamente una instancia de EC2 a una base de datos de RDS, consulte Configure automatic

network connectivity with an EC2 instance (Configuración de la conectividad automática de red con una instancia de EC2) en la Guía del usuario de Amazon RDS.

Cómo se configura automáticamente la conexión

Cuando se utiliza la consola de EC2 para configurar automáticamente la conexión entre una instancia de EC2 y una base de datos de RDS para permitir el tráfico entre ellas, la conexión se configura mediante grupos de seguridad.

Los grupos de seguridad se crean y se agregan automáticamente a la instancia de EC2 y a la base de datos de RDS de la siguiente manera:

- Amazon EC2 crea un grupo de seguridad denominado ec2-rds-***x*** y lo agrega a la instancia de EC2. Tiene una regla de salida que permite el tráfico a la base de datos al especificar rds-ec2-***x*** (el grupo de seguridad de la base de datos) como destino.
- Amazon RDS crea un grupo de seguridad denominado rds-ec2-***x*** y lo agrega a la base de datos. Tiene una regla de entrada que permite el tráfico desde la instancia de EC2 al especificar ec2-rds-***x*** (el grupo de seguridad de la instancia de EC2) como origen.

Los grupos de seguridad se hacen referencia entre sí como destino y origen, y solo permiten el tráfico en el puerto de la base de datos. Puede reutilizar estos grupos de seguridad de modo que cualquier base de datos con el grupo de seguridad rds-ec2-***x*** pueda comunicarse con cualquier instancia de EC2 con el grupo de seguridad ec2-rds-***x***.

Los nombres de los grupos de seguridad siguen un patrón. Para los grupos de seguridad creados por Amazon EC2, el patrón es ec2-rds-***x*** y, para los grupos de seguridad creados por Amazon RDS, el patrón es rds-ec2-***x***. ***x*** es un número que aumenta en 1 cada vez que se crea un nuevo grupo de seguridad automáticamente.

Tutorial: conexión de una instancia de Amazon EC2 a una base de datos de Amazon RDS

Objetivo del tutorial

El objetivo de este tutorial es que aprenda a configurar una conexión segura entre una instancia de Amazon EC2 y una base de datos de Amazon RDS con la AWS Management Console.

Hay distintas opciones para configurar la conexión. En este tutorial, se exploran las siguientes tres opciones:

- Opción 1: conexión automática de la instancia de EC2 a la base de datos de RDS con la consola de EC2

  Utilice la característica de conexión automática de la consola de EC2 para configurar automáticamente la conexión entre la instancia de EC2 y la base de datos de RDS y así permitir el tráfico entre la instancia de EC2 y la base de datos de RDS.

- Opción 2: conexión automática de la instancia de EC2 a la base de datos de RDS con la consola de RDS

  Utilice la característica de conexión automática de la consola de RDS para configurar automáticamente la conexión entre la instancia de EC2 y la base de datos de RDS para permitir el tráfico entre la instancia de EC2 y la base de datos de RDS.

- Opción 3: conexión manual de la instancia de EC2 a la base de datos de RDS imitando la característica de conexión automática

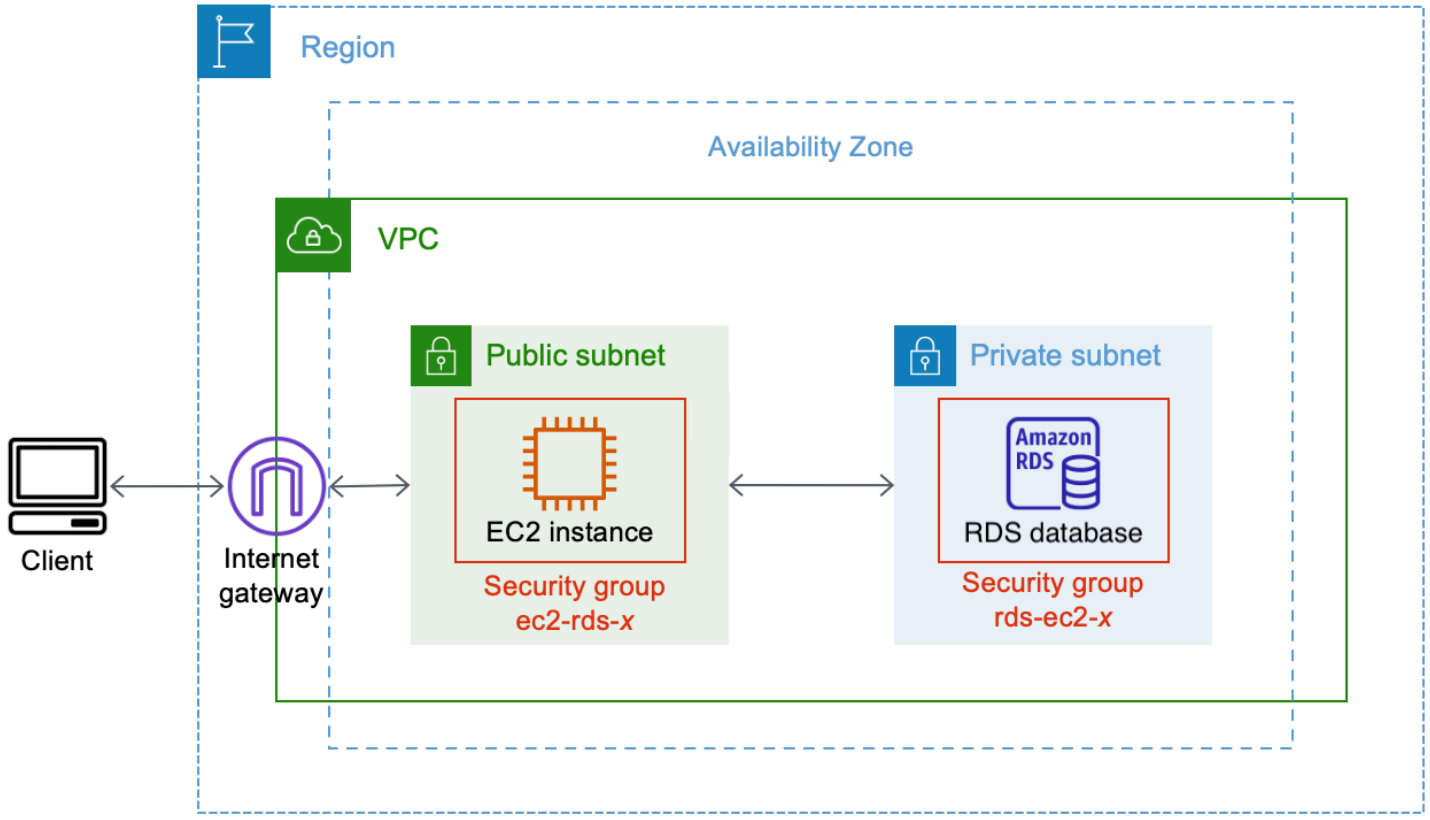
  Para configurar la conexión entre la instancia de EC2 y la base de datos de RDS, configure y asigne los grupos de seguridad para que reproduzcan la configuración que se crea automáticamente mediante la característica de conexión automática de las opciones 1 y 2.

Context

Como contexto para explicar por qué querría configurar una conexión entre una instancia de EC2 y una base de datos de RDS, tengamos en cuenta el siguiente escenario: en su sitio web se presenta un formulario para que los usuarios lo rellenen. Debe capturar los datos del formulario en una base de datos. Puede alojar el sitio web en una instancia de EC2 que se haya configurado como servidor web y capturar los datos del formulario en una base de datos de RDS. La instancia de EC2 y la base de datos de RDS deben estar conectadas entre sí para que los datos del formulario puedan ir de la instancia de EC2 a la base de datos de RDS. En este tutorial, se explica cómo configurar esa conexión. Tenga en cuenta que este es solo un ejemplo de un caso de uso para conectar una instancia de EC2 a una base de datos de RDS.

Arquitectura

En el siguiente diagrama, se muestran los recursos que se crean y la configuración de la arquitectura que se genera al completar todos los pasos de este tutorial.



En el diagrama, se muestran los siguientes recursos que va a crear:

- Creará una instancia de EC2 y una base de datos de RDS en la misma Región de AWS, VPC y zona de disponibilidad.
- Creará la instancia de EC2 en una subred pública.
- Creará la base de datos de RDS en una subred privada.

  Cuando se utiliza la consola de RDS para crear la base de datos de RDS y conectar automáticamente la instancia de EC2, la VPC, el grupo de subredes de base de datos y la configuración de acceso público de la base de datos se seleccionan automáticamente. La base de datos de RDS se crea automáticamente en una subred privada dentro de la misma VPC que la instancia de EC2.
- Los usuarios de Internet pueden conectarse a la instancia de EC2 mediante SSH o HTTP/HTTPS a través de una puerta de enlace de Internet.
- Los usuarios de Internet no pueden conectarse directamente a la base de datos RDS; solo la instancia de EC2 se conecta a la base de datos de RDS.

- Cuando se utiliza la característica de conexión automática para permitir el tráfico entre la instancia de EC2 y la base de datos de RDS, se crean y agregan automáticamente los siguientes grupos de seguridad:
  - Se crea el grupo de seguridad ec2-rds-***x*** y se agrega a la instancia de EC2. Tiene una regla de salida que hace referencia al grupo de seguridad rds-ec2-***x*** como destino. Esto permite que el tráfico de la instancia de EC2 llegue a la base de datos de RDS con el grupo de seguridad rds-ec2-***x***.
  - Se crea el grupo de seguridad rds-ec2-***x*** y se agrega a la base de datos de RDS. Tiene una regla de entrada que hace referencia al grupo de seguridad ec2-rds-***x*** como destino. Esto permite que el tráfico de la instancia de EC2 con el grupo de seguridad ec2-rds-***x*** llegue a la base de datos de RDS.

  Al usar grupos de seguridad independientes (uno para la instancia de EC2 y otro para la base de datos de RDS), tiene un mejor control de la seguridad de la instancia y la base de datos. Si tuviera que utilizar el mismo grupo de seguridad tanto en la instancia como en la base de datos y, a continuación, modificar el grupo de seguridad para adaptarlo, por ejemplo, solo a la base de datos, la modificación afectaría tanto a la instancia como a la base de datos. En otras palabras, si tuviera que utilizar un grupo de seguridad, podría modificar involuntariamente la seguridad de un recurso (ya sea la instancia o la base de datos) si se olvidara de que el grupo de seguridad ya estaba adjunto a él.

  Los grupos de seguridad que se crean automáticamente también respetan el privilegio mínimo, ya que solo permiten la conexión mutua para esta carga de trabajo en el puerto de la base de datos mediante la creación de un par de grupos de seguridad específico para la carga de trabajo.

Consideraciones

Tenga en cuenta lo siguiente al completar las tareas de este tutorial:

- Dos consolas: en este tutorial, utilizará las dos consolas siguientes:
  - Consola de Amazon EC2: utilizará la consola de EC2 para iniciar instancias, conectar automáticamente una instancia de EC2 a una base de datos de RDS y para la opción de configuración manual de la conexión mediante la creación de grupos de seguridad.
  - Consola de Amazon RDS: utilizará la consola de RDS para crear una base de datos de RDS y conectar automáticamente una instancia de EC2 a una base de datos de RDS.
- Una VPC: para poder usar la característica de conexión automática, la instancia de EC2 y la base de datos de RDS deben estar en la misma VPC.

Si tuviera que configurar manualmente la conexión entre la instancia de EC2 y la base de datos de RDS, podría iniciar la instancia de EC2 en una VPC y la base de datos de RDS en otra VPC; sin embargo, tendría que definir el enrutamiento y la configuración de la VPC adicionales. No se aborda este escenario en este tutorial.

- Una Región de AWS: la instancia de EC2 y la base de datos de RDS deben estar en la misma región.
- Dos grupos de seguridad: la conectividad entre la instancia de EC2 y la base de datos de RDS se configura mediante dos grupos de seguridad (un grupo de seguridad para la instancia de EC2 y un grupo de seguridad para la base de datos de RDS).

  Cuando se utiliza la característica de conexión automática de la consola de EC2 o de la consola de RDS para configurar la conectividad (opciones 1 y 2 de este tutorial), los grupos de seguridad se crean y asignan automáticamente a la instancia de EC2 y a la base de datos de RDS.

  Si no usa la característica de conexión automática, tendrá que crear y asignar los grupos de seguridad de forma manual. Puede hacerlo en la opción 3 de este tutorial.

Tiempo para completar el tutorial

30 minutos

Puede completar todo el tutorial de una vez o puede completarlo por tareas.

Costos

Al completar este tutorial, puede incurrir en costos por los recursos de AWS que cree.

Puede usar Amazon EC2 con el nivel gratuito siempre que su cuenta de AWS tenga menos de 12 meses de antigüedad y configure los recursos de acuerdo con los requisitos del nivel gratuito.

Incurrirá en gastos por transferencia de datos si la instancia de EC2 y la base de datos de RDS se encuentran en distintas zonas de disponibilidad. Para evitar incurrir en estos cargos, la instancia de EC2 y la base de datos de RDS deben estar en la misma zona de disponibilidad. Para obtener más información sobre las tarifas de transferencia de datos, consulte la sección Transferencia de datos en la página Precios de las instancias bajo demanda de Amazon EC2.

Para evitar incurrir en gastos después de completar el tutorial, asegúrese de eliminar los recursos si ya no los necesita. Para ver los pasos para eliminar los recursos, consulte Limpieza.

Opción 1: conexión automática de la instancia de EC2 a la base de datos de RDS con la consola de EC2

Objetivo

El objetivo de la opción 1 es explorar la característica de conexión automática de la consola de EC2 que configura automáticamente la conexión entre la instancia de EC2 y la base de datos de RDS para permitir el tráfico de la instancia de EC2 a la base de datos de RDS. En la opción 3, aprenderá a configurar la conexión de forma manual.

Antes de empezar

Para completar este tutorial, necesitará lo siguiente:

- Una base de datos de RDS que esté en la misma VPC que la instancia de EC2. Puede utilizar una base de datos de RDS existente o seguir los pasos de la tarea 1 para crear una nueva.
- Una instancia de EC2 que esté en la misma VPC que la base de datos de RDS. Puede utilizar una instancia de EC2 existente o seguir los pasos de la tarea 2 para crear una nueva.
- Permisos para llamar a las siguientes operaciones:
  - `ec2:AssociateRouteTable`
  - `ec2:AuthorizeSecurityGroupEgress`
  - `ec2:CreateRouteTable`
  - `ec2:CreateSecurityGroup`
  - `ec2:CreateSubnet`
  - `ec2:DescribeInstances`
  - `ec2:DescribeNetworkInterfaces`
  - `ec2:DescribeRouteTables`
  - `ec2:DescribeSecurityGroups`
  - `ec2:DescribeSubnets`
  - `ec2:ModifyNetworkInterfaceAttribute`
  - `ec2:RevokeSecurityGroupEgress`

Tareas para completar la opción 1

- Tarea 1: creación de una base de datos de RDS (opcional)
- Tarea 2: inicialización de una instancia de EC2 (opcional)

- Tarea 3: conexión automática de la instancia de EC2 a la base de datos de RDS
- Tarea 4: comprobación de la configuración de la conexión

Tarea 1: creación de una base de datos de RDS (opcional)

> **Note**
>
> El objetivo de este tutorial no es crear una base de datos de Amazon RDS. Si ya tiene una base de datos de RDS y desea utilizarla en este tutorial, puede omitir esta tarea.

Objetivo de la tarea

El objetivo de esta tarea es crear una base de datos de RDS para poder completar la tarea 3, en la que se configura la conexión entre la instancia de EC2 y la base de datos de RDS. Si tiene una base de datos de RDS que pueda utilizar, puede omitir esta tarea.

> **Important**
>
> Si usa una base de datos de RDS existente, asegúrese de que esté en la misma VPC que la instancia de EC2 para poder usar la característica de conexión automática.

Pasos para crear una base de datos de RDS

Siga los pasos que se indican a continuación para crear una base de datos de RDS.

Para ver una animación de estos pasos, consulte Ver animación: creación de una base de datos de RDS.

Configuración de la base de datos de RDS

Los pasos de esta tarea configuran la base de datos de RDS de la siguiente manera:

- Tipo de motor: MySQL
- Plantilla: nivel gratuito
- Identificador de la instancia de la base de datos: **`tutorial-database-1`**
- Clase de instancia de la base de datos: `db.t3.micro`

> **Important**
>
> En un entorno de producción, tiene que configurar la base de datos para que se ajuste a sus necesidades específicas.

Para crear una base de datos MySQL de RDS

1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el selector de regiones (en la parte superior derecha), elija una Región de AWS. La base de datos y la instancia de EC2 deben estar en la misma región para poder utilizar la característica de conexión automática de la consola de EC2.
3. En el panel, elija Create database (Crear base de datos).
4. En Choose a database creation method (Elegir un método de creación de base de datos), compruebe que la opción Standard Create (Creación estándar) esté seleccionada. Si elige Easy create (Creación sencilla), el selector de VPC no estará disponible. Debe asegurarse de que la base de datos esté en la misma VPC que la instancia de EC2 para poder utilizar la característica de conexión automática de la consola de EC2.
5. En Engine options (Opciones del motor), para Engine type (Tipo de motor), elija MySQL.
6. En Templates (Plantillas), elija una plantilla de ejemplo que se adapte a sus necesidades. Para este tutorial, elija Free tier (Nivel gratuito) y cree una base de datos sin costo alguno. Sin embargo, tenga en cuenta que el nivel gratuito solo está disponible si la cuenta tiene menos de 12 meses de antigüedad. Se aplican otras restricciones. Para obtener más información, seleccione el enlace Info (Información) en el cuadro Free tier (Nivel gratuito).
7. En Configuración, realice la siguiente operación:
   a. En DB instance identifier (Identificador de instancias de bases de datos), ingrese un nombre para la base de datos. En este tutorial, escriba **`tutorial-database-1`**.
   b. En Master username (Nombre de usuario maestro), deje el nombre predeterminado, que es **`admin`**.
   c. En Master password (Contraseña maestra), ingrese una contraseña que pueda recordar para este tutorial y, a continuación, en Confirm password (Confirmar contraseña), vuelva a escribirla.
8. En Instance configuration (Configuración de la instancia), para DB instance class (Clase de instancia de la base de datos), deje el valor predeterminado, que es db.t3.micro. Si la cuenta

tiene menos de 12 meses de antigüedad, puede utilizar esta clase de base de datos de forma gratuita. Se aplican otras restricciones. Para obtener más información, consulte Capa gratuita de AWS.

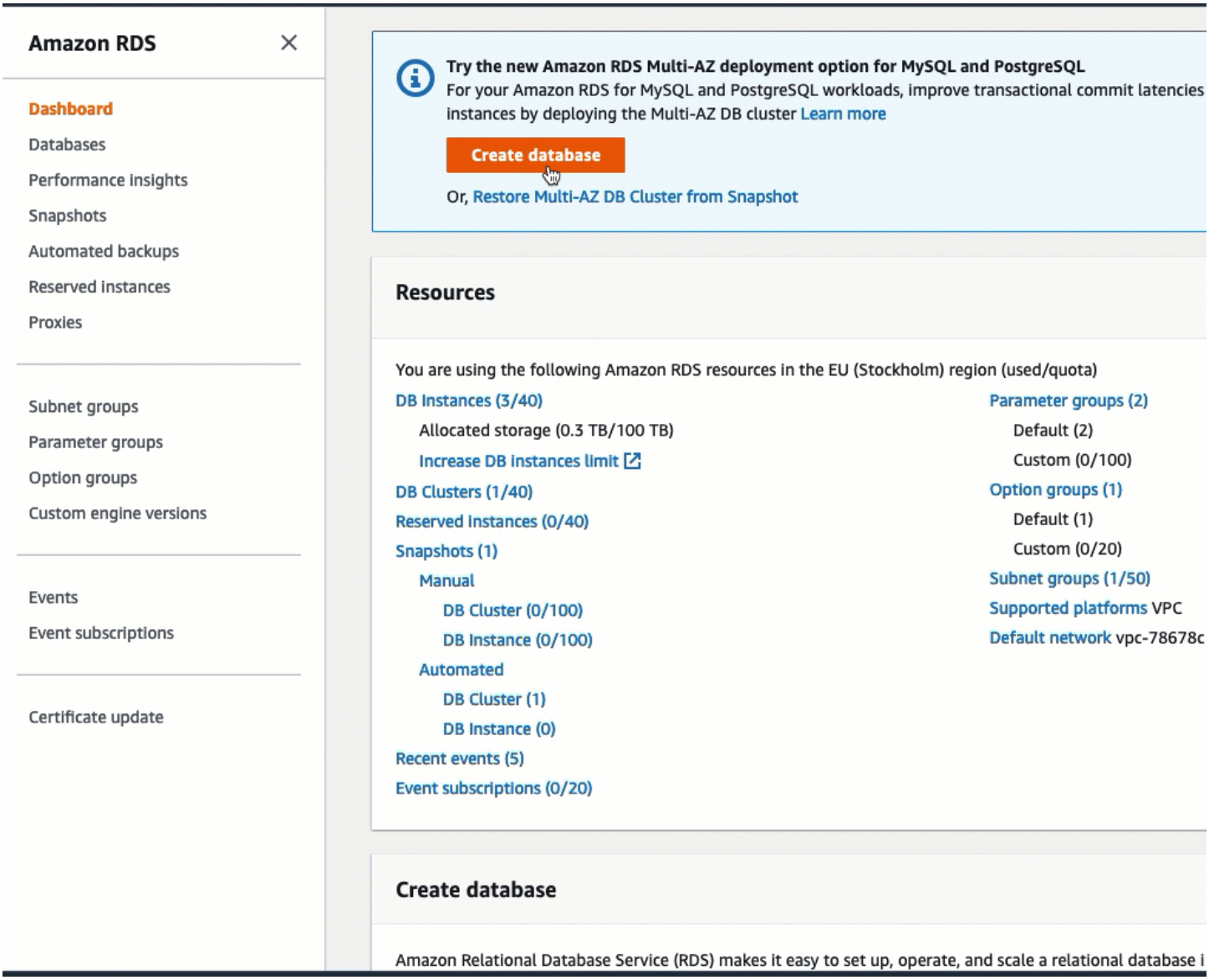
9. En Connectivity (Conectividad), en Compute resource (Recurso informático), elija Don't connect to an EC2 compute resource (No conectarse a un recurso informático de EC2) porque conectará la instancia de EC2 y la base de datos de RDS más adelante en la tarea 3.

   (Más adelante, en la opción 2 de este tutorial, para probar la característica de conexión automática de la consola de RDS, seleccionará Connect to an EC2 compute resource [Conectarse a un recurso informático de EC2]).

10. En Virtual private cloud (VPC) (Nube privada virtual [VPC]), seleccione una VPC. La VPC debe tener un grupo de subred de base de datos. Para poder usar la característica de conexión automática, la instancia de EC2 y la base de datos de RDS deben estar en la misma VPC.
11. Para todos los demás campos de esta página, mantenga los valores predeterminados.
12. Seleccione Crear base de datos.

    En la pantalla Databases (Bases de datos), Status (Estado) de la nueva base de datos es Creating (En creación) hasta que la base de datos esté lista para usarse. Cuando el estado cambie a Available (Disponible), podrá conectarse a la base de datos. Según la clase de la base de datos y la cantidad de almacenamiento, es posible que la nueva base de datos tarde hasta 20 minutos en estar disponible.

Ver animación: creación de una base de datos de RDS



Ya lo tiene todo listo para Tarea 2: inicialización de una instancia de EC2 (opcional).

Tarea 2: inicialización de una instancia de EC2 (opcional)

> **Note**
>
> El objetivo de este tutorial no es iniciar una instancia. Si ya tiene una instancia de Amazon EC2 y desea utilizarla en este tutorial, puede omitir esta tarea.

Objetivo de la tarea

El objetivo de esta tarea es iniciar una instancia de EC2 para poder completar la tarea 3, en la que se configura la conexión entre la instancia de EC2 y la base de datos de Amazon RDS. Si tiene una instancia de EC2 que pueda utilizar, puede omitir esta tarea.

> **Important**
>
> Si usa una instancia de EC2 existente, asegúrese de que esté en la misma VPC que la base de datos de RDS para poder usar la característica de conexión automática.

Pasos para iniciar una instancia de EC2

Para este tutorial, siga los pasos que se indican a continuación para iniciar una instancia de EC2.

Para ver una animación de estos pasos, consulte Ver animación: inicialización de una instancia de EC2.

Configuración de instancias de EC2

Los pasos de esta tarea configuran la instancia de EC2 de la siguiente manera:

- Nombre de instancia: **`tutorial-instance-1`**
- AMI: Amazon Linux 2
- Tipo de instancia: `t2.micro`
- Asignar automáticamente IP pública: habilitado
- Grupo de seguridad con las tres reglas siguientes:
  - Permitir SSH desde su dirección IP
  - Permitir el tráfico HTTPS desde cualquier lugar
  - Permitir el tráfico HTTP desde cualquier lugar

> **Important**
>
> En un entorno de producción, tiene que configurar la instancia para que se ajuste a sus necesidades específicas.

Para iniciar una instancia de EC2

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el selector de regiones (en la parte superior derecha), elija una Región de AWS. La instancia y la base de datos de RDS deben estar en la misma región para poder utilizar la característica de conexión automática de la consola de EC2.
3. En el panel de EC2, elija Launch Instance (iniciar instancia).
4. En Name and tags (Nombre y etiquetas), ingrese un nombre para identificar la instancia en Name (Nombre). En este tutorial, asigne el nombre **`tutorial-instance-1`** a la instancia. Si bien el nombre de la instancia no es obligatorio, le ayudará a identificarla más fácilmente cuando la seleccione en la consola de EC2.
5. En Application and OS Images (Imágenes de aplicaciones y sistema operativo), elija una AMI que se adapte a las necesidades de su servidor web. En este tutorial, se utiliza Amazon Linux 2.
6. En Instance type (Tipo de instancia), para Instance type (Tipo de instancia), seleccione uno que se adapte a las necesidades de su servidor web. En este tutorial se utiliza un `t2.micro`.

   > **Note**
   >
   > Puede usar Amazon EC2 con el nivel gratuito siempre que su cuenta de AWS tenga menos de 12 meses de antigüedad y elija un tipo de instancia `t2.micro` (o `t3.micro` en las regiones en las que `t2.micro` no esté disponible).

7. En Key pair (login) (Par de claves [inicio de sesión]), para Key pair name (Nombre del par de claves), elija el par de claves.
8. En Network settings (Configuración de red), haga lo siguiente:

   a. En Network (Red) y Subnet (Subred), si no hizo cambios en la VPC ni las subredes predeterminadas, puede conservar la configuración predeterminada.

      Si hizo cambios en la VPC o las subredes predeterminadas, compruebe lo siguiente:

      i. Para poder usar la característica de conexión automática, la instancia y la base de datos de RDS deben estar en la misma VPC. De forma predeterminada, solo tiene una VPC.

      ii. La VPC en la que va a iniciar la instancia debe tener una puerta de enlace de Internet conectada para que pueda acceder al servidor web desde Internet. La VPC predeterminada se configura automáticamente con una puerta de enlace de Internet.

iii. Para garantizar que la instancia reciba una dirección IP pública, en Auto-assign public IP (Asignar automáticamente IP pública), compruebe que la opción Enable (Habilitar) esté seleccionada. Si la opción Disable (Deshabilitar) está seleccionada, elija Edit (Editar) (a la derecha de Network Settings [Configuración de red]) y, a continuación, en Auto-assign public IP (Asignar automáticamente IP pública), elija Enable (Habilitar).

b. Para conectarse a la instancia mediante SSH, necesita una regla de grupo de seguridad que autorice el tráfico SSH (Linux) o RDP (Windows) desde la dirección IPv4 pública del equipo. De forma predeterminada, al iniciar una instancia, se crea un nuevo grupo de seguridad con una regla que permite el tráfico SSH de entrada desde cualquier lugar.

   Para asegurarse de que solo su dirección IP pueda conectarse a la instancia, en Firewall (security groups) (Firewall [grupos de seguridad]), en la lista desplegable situada junto a la casilla Allow SSH traffic from (Permitir tráfico SSH desde), seleccione My IP (Mi IP).

c. Para permitir el tráfico de Internet a la instancia, seleccione las siguientes casillas:

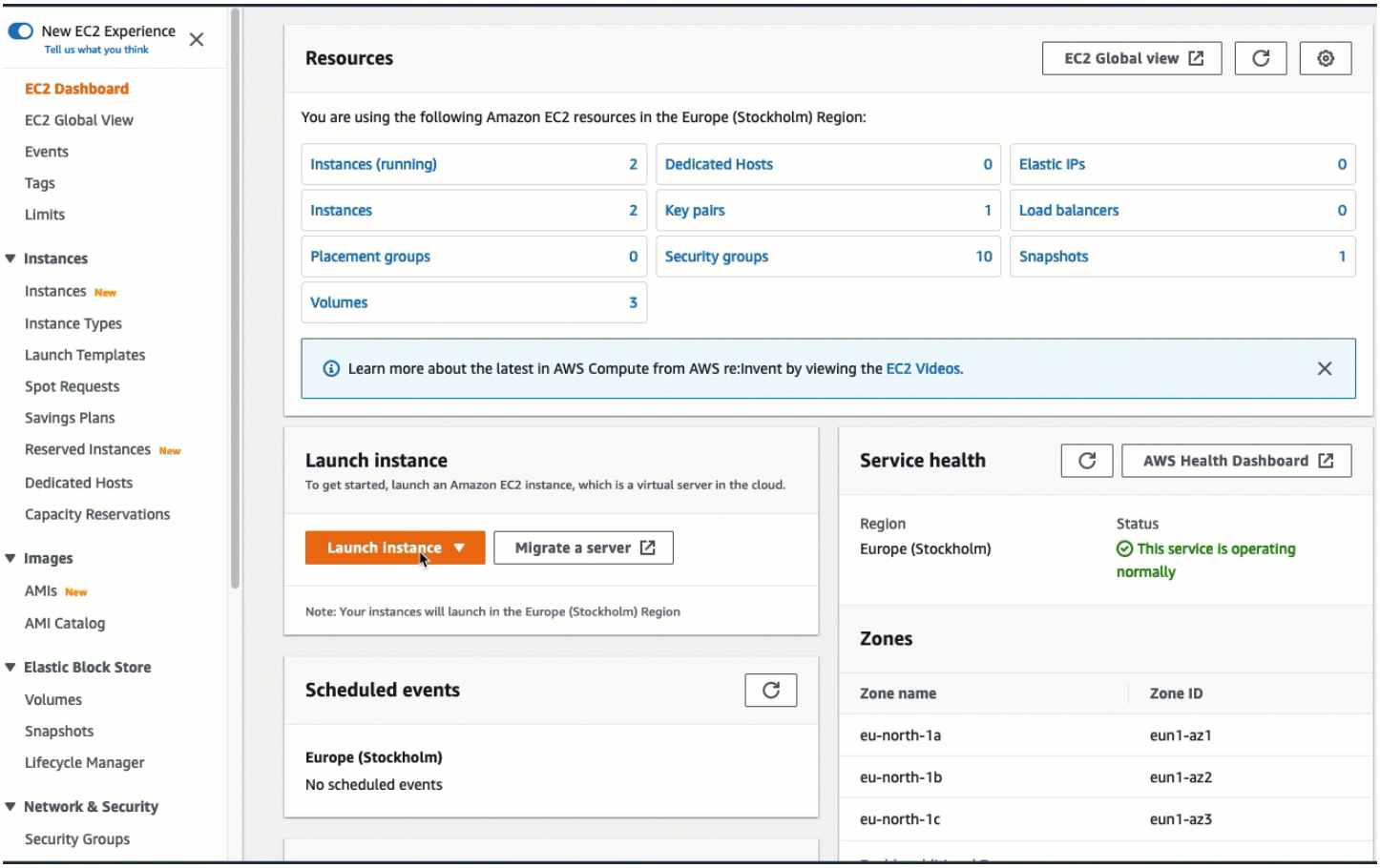
   - Allow HTTPs traffic from the internet (Permitir el tráfico HTTPS desde Internet)
   - Allow HTTP traffic from the internet (Permitir el tráfico HTTP desde Internet)

9. En el panel Summary (Resumen), revise la configuración de la instancia y, a continuación, elija Launch instance (iniciar instancia).
10. Mantenga abierta la página de confirmación. La necesitará en la siguiente tarea cuando conecte automáticamente la instancia a la base de datos.

    Si se produce un error al iniciar la instancia o el estado pasa inmediatamente a `terminated` en lugar de `running`, consulte Solucionar problemas de lanzamiento de instancias.

Para obtener más información acerca de cómo iniciar una instancia, consulte Lance una instancia con el nuevo asistente de inicialización de instancias.

Ver animación: inicialización de una instancia de EC2



Ya lo tiene todo listo para Tarea 3: conexión automática de la instancia de EC2 a la base de datos de RDS.

Tarea 3: conexión automática de la instancia de EC2 a la base de datos de RDS

Objetivo de la tarea

El objetivo de esta tarea es utilizar la característica de conexión automática de la consola de EC2 para configurar automáticamente la conexión entre la instancia de EC2 y la base de datos de RDS.

Pasos para conectar la instancia de EC2 y la base de datos de RDS

Siga los pasos que se indican a continuación para conectar la instancia de EC2 y la base de datos de RDS mediante la característica automática de la consola de EC2.

Para ver una animación de estos pasos, consulte Ver animación: conexión automática de una instancia de EC2 recién iniciada a una base de datos de RDS.

Para conectar automáticamente una instancia de EC2 a una base de datos de RDS mediante la consola de EC2

1. En la página de confirmación de la inicialización de la instancia (debería estar abierta desde la tarea anterior), elija Connect an RDS database (Conectar una base de datos de RDS).

   Si cerró la página de confirmación, siga estos pasos:

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

   b. En el panel de navegación, seleccione Instances (Instancia[s]).

   c. Seleccione la instancia de EC2 que acaba de crear y, a continuación, elija Actions (Acciones), Networking (Redes), Connect RDS database (Conectar la base de datos de RDS).

      Si Connect RDS database (Conectar la base de datos de RDS) no está disponible, compruebe que el estado de la instancia de EC2 sea Running (En ejecución).

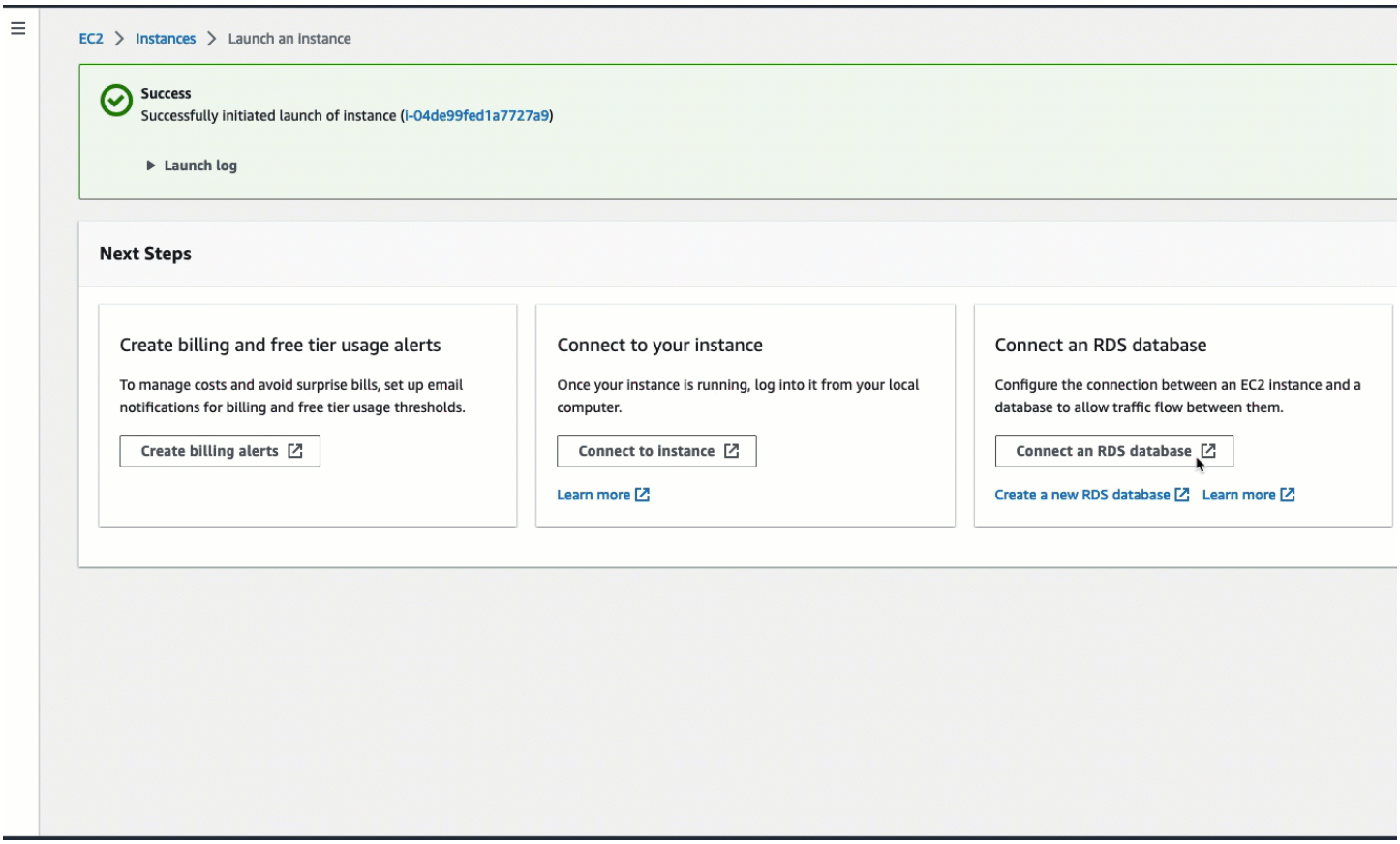
2. En Database role (Rol de base de datos), elija Instance (instancia). En este caso, Instance (instancia) hace referencia a la instancia de la base de datos.

3. En RDS database (Base de datos de RDS), elija la base de datos de RDS que creó en la tarea 1.

   > **Note**
   >
   > La instancia de EC2 y la base de datos de RDS deben estar en la misma VPC para poder conectarse entre sí.

4. Elija Conectar.

Ver animación: conexión automática de una instancia de EC2 recién iniciada a una base de datos de RDS



Ya lo tiene todo listo para Tarea 4: comprobación de la configuración de la conexión.

Tarea 4: comprobación de la configuración de la conexión

Objetivo de la tarea

El objetivo de esta tarea es comprobar que los dos grupos de seguridad se crearon y asignaron a la instancia y a la base de datos.

Cuando se utiliza la característica de conexión automática de la consola de EC2 para configurar la conectividad, los grupos de seguridad se crean y asignan automáticamente a la instancia y a la base de datos, tal como se indica a continuación:

- Se crea el grupo de seguridad rds-ec2-*x* y se agrega a la base de datos de RDS. Tiene una regla de entrada que hace referencia al grupo de seguridad ec2-rds-*x* como destino. Esto permite que el tráfico de la instancia de EC2 con el grupo de seguridad ec2-rds-*x* llegue a la base de datos de RDS.

- Se crea el grupo de seguridad ec2-rds-*x* y se agrega a la instancia de EC2. Tiene una regla de salida que hace referencia al grupo de seguridad rds-ec2-*x* como destino. Esto permite que el tráfico de la instancia de EC2 llegue a la base de datos de RDS con el grupo de seguridad rds-ec2-*x*.

Pasos para comprobar la configuración de la conexión

Siga los pasos que se indican a continuación para comprobar la configuración de la conexión.

Para ver una animación de estos pasos, consulte Ver animación: comprobación de la configuración de la conexión.

Para comprobar la configuración de la conexión mediante la consola

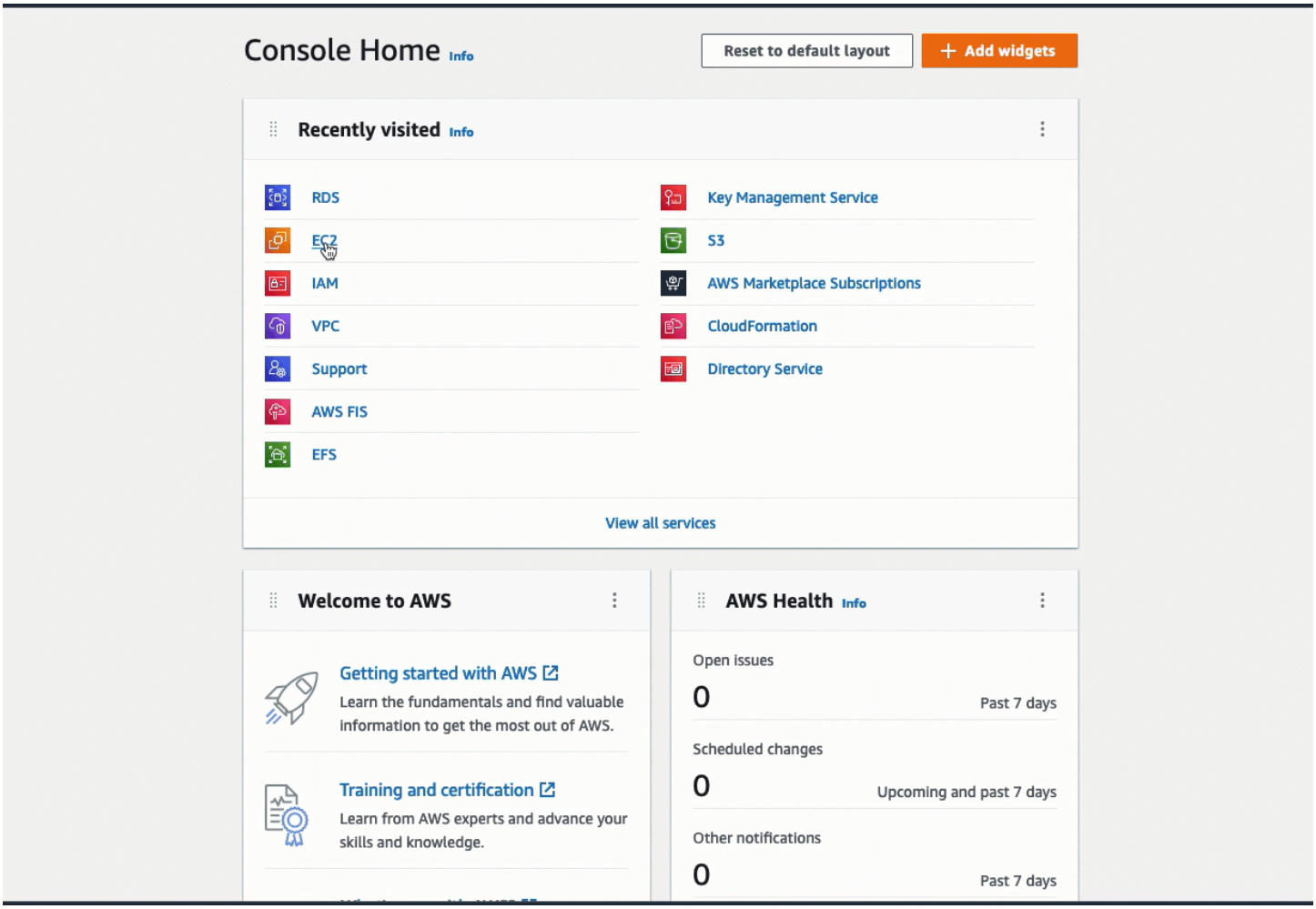
1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos).
3. Elija la base de datos de RDS que creó para este tutorial.
4. En la pestaña Connectivity & security (Conectividad y seguridad), en Security (Seguridad), VPC security groups (Grupos de seguridad de VPC), compruebe que aparezca un grupo de seguridad denominado rds-ec2-*x*.
5. Elija el grupo de seguridad rds-ec2-*x*. Se abre la pantalla Security Groups (Grupos de seguridad) de la consola de EC2.
6. Elija el grupo de seguridad rds-ec2-*x* para abrirlo.
7. Elija la pestaña Reglas de entrada.
8. Compruebe que exista la siguiente regla de grupo de seguridad, como se muestra a continuación:
   - Tipo: MySQL/Aurora
   - Intervalo de puertos: 3306
   - Origen: *sg-0987654321example*/ec2-rds-*x*. Este es el grupo de seguridad que se asigna a la instancia de EC2 que comprobó en los pasos anteriores.
   - Descripción: Rule to allow connections from EC2 instances with *sg-1234567890example* attached (Regla para permitir conexiones desde instancias de EC2 con sg-1234567890example adjunto)
9. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.

10. En el panel de navegación, seleccione Instances (Instancia[s]).
11. Elija la instancia de EC2 que seleccionó para conectarse a la base de datos de RDS en la tarea anterior y elija la pestaña Security (Seguridad).
12. En Security details (Detalles de seguridad), Security groups (Grupos de seguridad), compruebe que haya un grupo de seguridad denominado ec2-rds-*x* en la lista. *x* es un número.
13. Elija el grupo de seguridad ec2-rds-*x* para abrirlo.
14. Elija la pestaña Outbound rules (Reglas de salida).
15. Compruebe que exista la siguiente regla de grupo de seguridad, como se muestra a continuación:

    - Tipo: MySQL/Aurora
    - Intervalo de puertos: 3306
    - Destino: *sg-1234567890example*/rds-ec2-*x*
    - Descripción: regla para permitir conexiones a **database-tutorial** desde cualquier instancia a la que esté adjunto este grupo de seguridad

Al comprobar que estos grupos de seguridad y reglas de grupos de seguridad existen y están asignados a la base de datos de RDS y a la instancia de EC2 tal como se describe en este procedimiento, puede comprobar que la conexión se configuró automáticamente mediante la característica de conexión automática.

Ver animación: comprobación de la configuración de la conexión



Completó la opción 1 de este tutorial. Ahora puede completar la opción 2, que le enseña cómo usar la consola de RDS para conectar automáticamente una instancia de EC2 a una base de datos de RDS, o puede completar la opción 3, que le enseña cómo configurar manualmente los grupos de seguridad que se crearon automáticamente en la opción 1.

Opción 2: conexión automática de la instancia de EC2 a la base de datos de RDS con la consola de RDS

Objetivo

El objetivo de la opción 2 es explorar la característica de conexión automática de la consola de RDS que configura automáticamente la conexión entre la instancia de EC2 y la base de datos de RDS para permitir el tráfico de la instancia de EC2 a la base de datos de RDS. En la opción 3, aprenderá a configurar la conexión de forma manual.

Antes de empezar

Para completar este tutorial, necesitará lo siguiente:

- Una instancia de EC2 que esté en la misma VPC que la base de datos de RDS. Puede utilizar una instancia de EC2 existente o seguir los pasos de la tarea 1 para crear una instancia nueva.
- Permisos para llamar a las siguientes operaciones:
  - `ec2:AssociateRouteTable`
  - `ec2:AuthorizeSecurityGroupEgress`
  - `ec2:CreateRouteTable`
  - `ec2:CreateSecurityGroup`
  - `ec2:CreateSubnet`
  - `ec2:DescribeInstances`
  - `ec2:DescribeNetworkInterfaces`
  - `ec2:DescribeRouteTables`
  - `ec2:DescribeSecurityGroups`
  - `ec2:DescribeSubnets`
  - `ec2:ModifyNetworkInterfaceAttribute`
  - `ec2:RevokeSecurityGroupEgress`

Tareas para completar la opción 2

- Tarea 1: inicialización de una instancia de EC2 (opcional)
- Tarea 2: creación de una base de datos de RDS y conexión automática a la instancia de EC2
- Tarea 3: comprobación de la configuración de la conexión

Tarea 1: inicialización de una instancia de EC2 (opcional)

> **Note**
>
> El objetivo de este tutorial no es iniciar una instancia. Si ya tiene una instancia de Amazon EC2 y desea utilizarla en este tutorial, puede omitir esta tarea.

Objetivo de la tarea

El objetivo de esta tarea es iniciar una instancia de EC2 para poder completar la tarea 2, en la que se configura la conexión entre la instancia de EC2 y la base de datos de Amazon RDS. Si tiene una instancia de EC2 que pueda utilizar, puede omitir esta tarea.

Pasos para iniciar una instancia de EC2

Para este tutorial, siga los pasos que se indican a continuación para iniciar una instancia de EC2.

Para ver una animación de estos pasos, consulte Ver animación: inicialización de una instancia de EC2.

Configuración de instancias de EC2

Los pasos de esta tarea configuran la instancia de EC2 de la siguiente manera:

- Nombre de instancia: **`tutorial-instance-2`**
- AMI: Amazon Linux 2
- Tipo de instancia: `t2.micro`
- Asignar automáticamente IP pública: habilitado
- Grupo de seguridad con las tres reglas siguientes:
  - Permitir SSH desde su dirección IP
  - Permitir el tráfico HTTPS desde cualquier lugar
  - Permitir el tráfico HTTP desde cualquier lugar

> **Important**
>
> En un entorno de producción, tiene que configurar la instancia para que se ajuste a sus necesidades específicas.

Para iniciar una instancia de EC2

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de EC2, elija Launch Instance (iniciar instancia).
3. En Name and tags (Nombre y etiquetas), ingrese un nombre para identificar la instancia en Name (Nombre). En este tutorial, asigne el nombre **`tutorial-instance-2`** a la instancia. Si

bien el nombre de la instancia no es obligatorio, le ayudará a identificarla más fácilmente cuando la seleccione en la consola de RDS.

4. En Application and OS Images (Imágenes de aplicaciones y sistema operativo), elija una AMI que se adapte a las necesidades de su servidor web. En este tutorial, se utiliza Amazon Linux.
5. En Instance type (Tipo de instancia), para Instance type (Tipo de instancia), seleccione uno que se adapte a las necesidades de su servidor web. En este tutorial se utiliza un `t2.micro`.

   > **Note**
   >
   > Puede usar Amazon EC2 con el nivel gratuito siempre que su cuenta de AWS tenga menos de 12 meses de antigüedad y elija un tipo de instancia `t2.micro` (o `t3.micro` en las regiones en las que `t2.micro` no esté disponible).

6. En Key pair (login) (Par de claves [inicio de sesión]), para Key pair name (Nombre del par de claves), elija el par de claves.
7. En Network settings (Configuración de red), haga lo siguiente:

   a. En Network (Red) y Subnet (Subred), si no hizo cambios en la VPC ni las subredes predeterminadas, puede conservar la configuración predeterminada.

      Si hizo cambios en la VPC o las subredes predeterminadas, compruebe lo siguiente:

      i. Para poder usar la configuración de conexión automática, la instancia y la base de datos de RDS deben estar en la misma VPC. De forma predeterminada, solo tiene una VPC.

      ii. La VPC en la que va a iniciar la instancia debe tener una puerta de enlace de Internet conectada para que pueda acceder al servidor web desde Internet. La VPC predeterminada se configura automáticamente con una puerta de enlace de Internet.

      iii. Para garantizar que la instancia reciba una dirección IP pública, en Auto-assign public IP (Asignar automáticamente IP pública), compruebe que la opción Enable (Habilitar) esté seleccionada. Si la opción Disable (Deshabilitar) está seleccionada, elija Edit (Editar) (a la derecha de Network Settings [Configuración de red]) y, a continuación, en Auto-assign public IP (Asignar automáticamente IP pública), elija Enable (Habilitar).

   b. Para conectarse a la instancia mediante SSH, necesita una regla de grupo de seguridad que autorice el tráfico SSH (Linux) o RDP (Windows) desde la dirección IPv4 pública del equipo. De forma predeterminada, al iniciar una instancia, se crea un nuevo grupo de seguridad con una regla que permite el tráfico SSH de entrada desde cualquier lugar.

Para asegurarse de que solo su dirección IP pueda conectarse a la instancia, en Firewall (security groups) (Firewall [grupos de seguridad]), en la lista desplegable situada junto a la casilla Allow SSH traffic from (Permitir tráfico SSH desde), seleccione My IP (Mi IP).

c. Para permitir el tráfico de Internet a la instancia, seleccione las siguientes casillas:

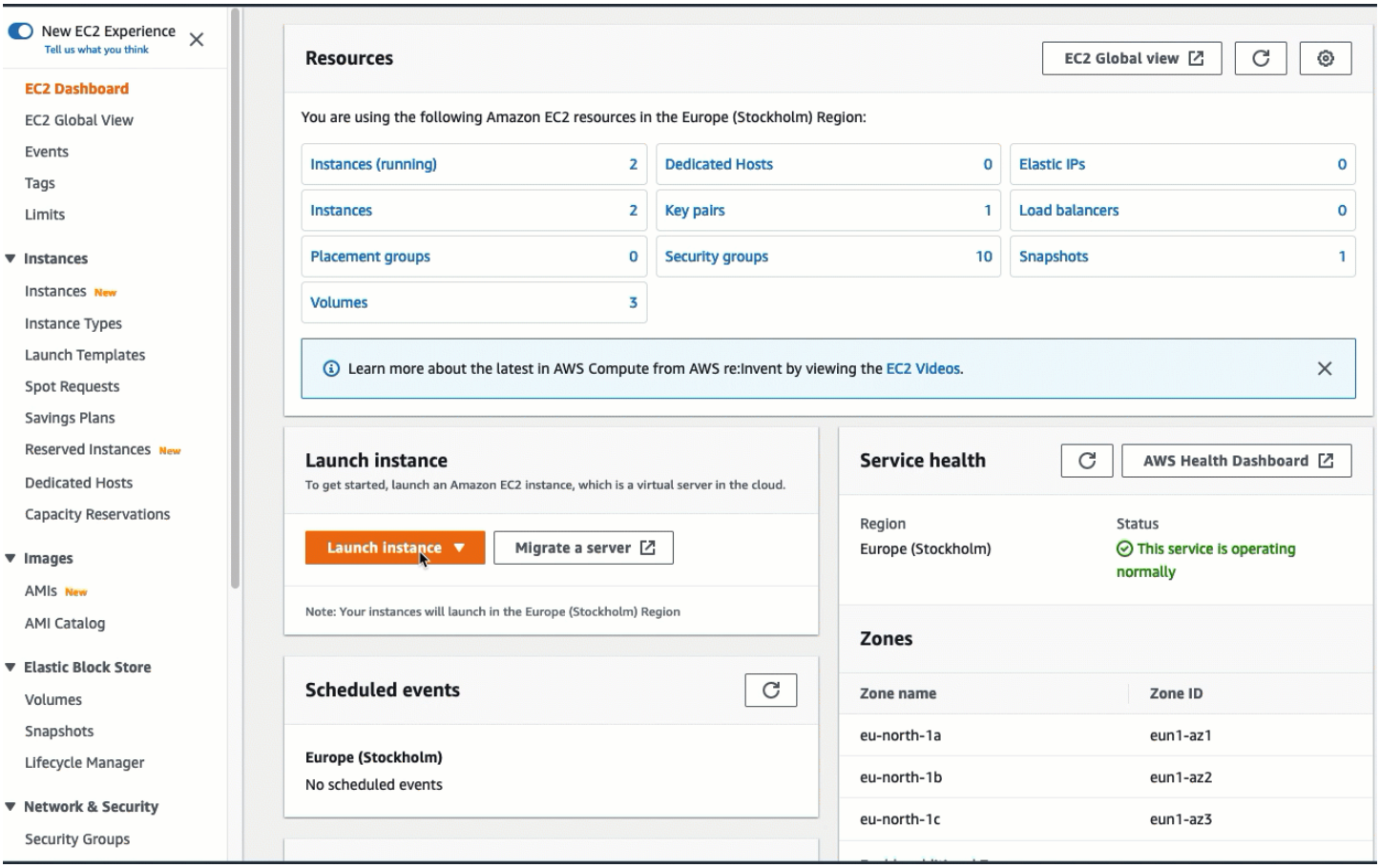
- Allow HTTPs traffic from the internet (Permitir el tráfico HTTPS desde Internet)
- Allow HTTP traffic from the internet (Permitir el tráfico HTTP desde Internet)

8. En el panel Summary (Resumen), revise la configuración de la instancia y, a continuación, elija Launch instance (iniciar instancia).
9. Elija Ver todas las instancias para cerrar la página de confirmación y volver a la consola. El estado inicial de la instancia será `pending` y, a continuación, pasará a `running`.

   Si se produce un error al iniciar la instancia o el estado pasa inmediatamente a `terminated` en lugar de `running`, consulte Solucionar problemas de lanzamiento de instancias.

Para obtener más información acerca de cómo iniciar una instancia, consulte Lance una instancia con el nuevo asistente de inicialización de instancias.

Ver animación: inicialización de una instancia de EC2



Ya lo tiene todo listo para Tarea 2: creación de una base de datos de RDS y conexión automática a la instancia de EC2.

Tarea 2: creación de una base de datos de RDS y conexión automática a la instancia de EC2

Objetivo de la tarea

El objetivo de esta tarea es crear una base de datos de RDS y usar la característica de conexión automática de la consola de RDS para configurar automáticamente la conexión entre la instancia de EC2 y la base de datos de RDS.

Pasos para crear una base de datos de RDS

Siga los pasos que se indican a continuación para crear una base de datos de RDS y conectarla a la instancia de EC2 mediante la característica automática de la consola de RDS.

Para ver una animación de estos pasos, consulte Ver animación: creación de una base de datos de RDS y conexión automática a una instancia de EC2.

Configuración de la instancia de la base de datos

Los pasos de esta tarea configuran la instancia de la base de datos de la siguiente manera:

- Tipo de motor: MySQL
- Plantilla: nivel gratuito
- Identificador de la instancia de la base de datos: **`tutorial-database`**
- Clase de instancia de la base de datos: `db.t3.micro`

> **Important**
>
> En un entorno de producción, tiene que configurar la instancia para que se ajuste a sus necesidades específicas.

Para crear una base de datos de RDS y conectarla automáticamente a una instancia de EC2

1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el selector de regiones (en la parte superior derecha), elija la Región de AWS en la que creó la instancia de EC2. La instancia de EC2 y la base de datos de RDS deben estar en la misma región.
3. En el panel, elija Create database (Crear base de datos).
4. En Choose a database creation method (Elegir un método de creación de base de datos), compruebe que la opción Standard Create (Creación estándar) esté seleccionada. Si elige Easy create (Creación sencilla), la característica de conexión automática no estará disponible.
5. En Engine options (Opciones del motor), para Engine type (Tipo de motor), elija MySQL.
6. En Templates (Plantillas), elija una plantilla de ejemplo que se adapte a sus necesidades. Para este tutorial, elija Free tier (Nivel gratuito) para crear una base de datos de RDS sin costo alguno. Sin embargo, tenga en cuenta que el nivel gratuito solo está disponible si la cuenta tiene menos de 12 meses de antigüedad. Se aplican otras restricciones. Para obtener más información, seleccione el enlace Info (Información) en el cuadro Free tier (Nivel gratuito).
7. En Configuración, realice la siguiente operación:

    a. En DB instance identifier (Identificador de instancias de bases de datos), ingrese un nombre para la base de datos. En este tutorial, escriba **`tutorial-database`**.

b. En Master username (Nombre de usuario maestro), deje el nombre predeterminado, que es **`admin`**.

c. En Master password (Contraseña maestra), ingrese una contraseña que pueda recordar para este tutorial y, a continuación, en Confirm password (Confirmar contraseña), vuelva a escribirla.

8. En Instance configuration (Configuración de la instancia), para DB instance class (Clase de instancia de la base de datos), deje el valor predeterminado, que es db.t3.micro. Si la cuenta tiene menos de 12 meses de antigüedad, puede utilizar esta instancia de forma gratuita. Se aplican otras restricciones. Para obtener más información, consulte Capa gratuita de AWS.

9. En Connectivity (Conectividad), en Compute resource (Recurso informático), elija Connect to an EC2 compute resource (Conectarse a un recurso informático de EC2). Esta es la característica de conexión automática de la consola de RDS.

10. En EC2 instance (instancia de EC2), elija la instancia de EC2 a la que desea conectarse. Para los fines de este tutorial, puede elegir la instancia que creó en la tarea anterior, con el nombre **`tutorial-instance`**, o elegir otra instancia existente. Si no ve la instancia en la lista, elija el icono de actualización que se encuentra a la derecha de Connectivity (Conectividad).

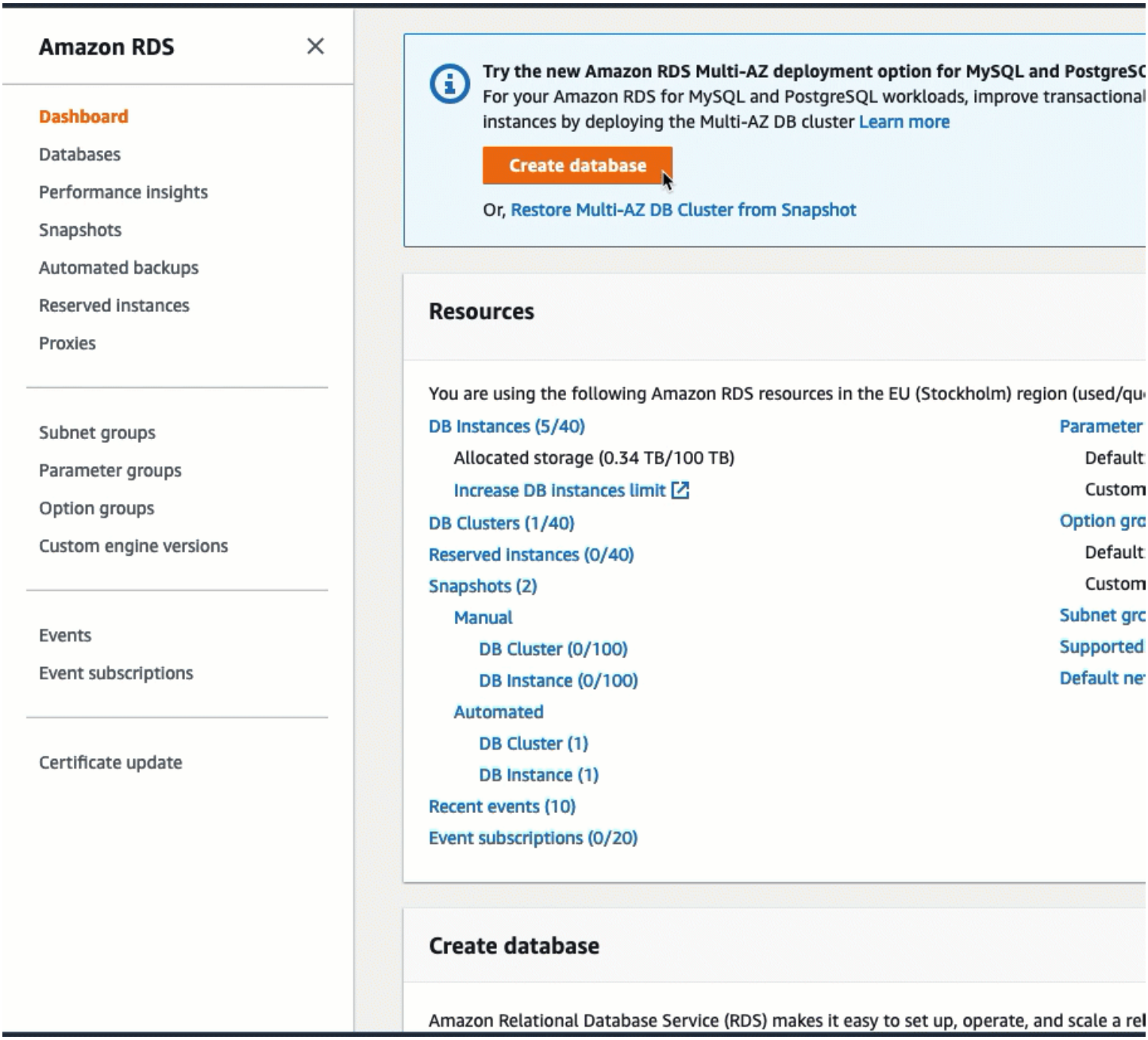
    Cuando se utiliza la característica de conexión automática, se agrega un grupo de seguridad a esta instancia de EC2 y otro, a la base de datos de RDS. Los grupos de seguridad se configuran automáticamente para permitir el tráfico entre la instancia de EC2 y la base de datos de RDS. En la siguiente tarea, comprobará que los grupos de seguridad se crearon y asignaron a la instancia de EC2 y a la base de datos de RDS.

11. Seleccione Crear base de datos.

    En la pantalla Databases (Bases de datos), Status (Estado) de la nueva base de datos es Creating (En creación) hasta que la base de datos esté lista para usarse. Cuando el estado cambie a Available (Disponible), podrá conectarse a la base de datos. Según la clase de la base de datos y la cantidad de almacenamiento, es posible que la nueva base de datos tarde hasta 20 minutos en estar disponible.

Para obtener más información, consulte Configure automatic network connectivity with an EC2 instance (Configuración de la conectividad automática de red con una instancia de EC2) en la Guía del usuario de Amazon RDS.

Ver animación: creación de una base de datos de RDS y conexión automática a una instancia de EC2



Ya lo tiene todo listo para Tarea 3: comprobación de la configuración de la conexión.

Tarea 3: comprobación de la configuración de la conexión

Objetivo de la tarea

El objetivo de esta tarea es comprobar que los dos grupos de seguridad se crearon y asignaron a la instancia y a la base de datos.

Cuando se utiliza la característica de conexión automática de la consola de RDS para configurar la conectividad, los grupos de seguridad se crean y asignan automáticamente a la instancia y a la base de datos, tal como se indica a continuación:

- Se crea el grupo de seguridad rds-ec2-***x*** y se agrega a la base de datos de RDS. Tiene una regla de entrada que hace referencia al grupo de seguridad ec2-rds-***x*** como destino. Esto permite que el tráfico de la instancia de EC2 con el grupo de seguridad ec2-rds-***x*** llegue a la base de datos de RDS.
- Se crea el grupo de seguridad ec2-rds-***x*** y se agrega a la instancia de EC2. Tiene una regla de salida que hace referencia al grupo de seguridad rds-ec2-***x*** como destino. Esto permite que el tráfico de la instancia de EC2 llegue a la base de datos de RDS con el grupo de seguridad rds-ec2-***x***.

Pasos para comprobar la configuración de la conexión

Siga los pasos que se indican a continuación para comprobar la configuración de la conexión.

Para ver una animación de estos pasos, consulte Ver animación: comprobación de la configuración de la conexión.

Para comprobar la configuración de la conexión mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Elija la instancia de EC2 que seleccionó para conectarse a la base de datos de RDS en la tarea anterior y elija la pestaña Security (Seguridad).
4. En Security details (Detalles de seguridad), Security groups (Grupos de seguridad), compruebe que haya un grupo de seguridad denominado ec2-rds-***x*** en la lista. *x* es un número.
5. Elija el grupo de seguridad ec2-rds-***x*** para abrirlo.
6. Elija la pestaña Outbound rules (Reglas de salida).
7. Compruebe que exista la siguiente regla de grupo de seguridad, como se muestra a continuación:
   - Tipo: MySQL/Aurora
   - Intervalo de puertos: 3306
   - Destino: ***sg-1234567890example***/rds-ec2-***x***

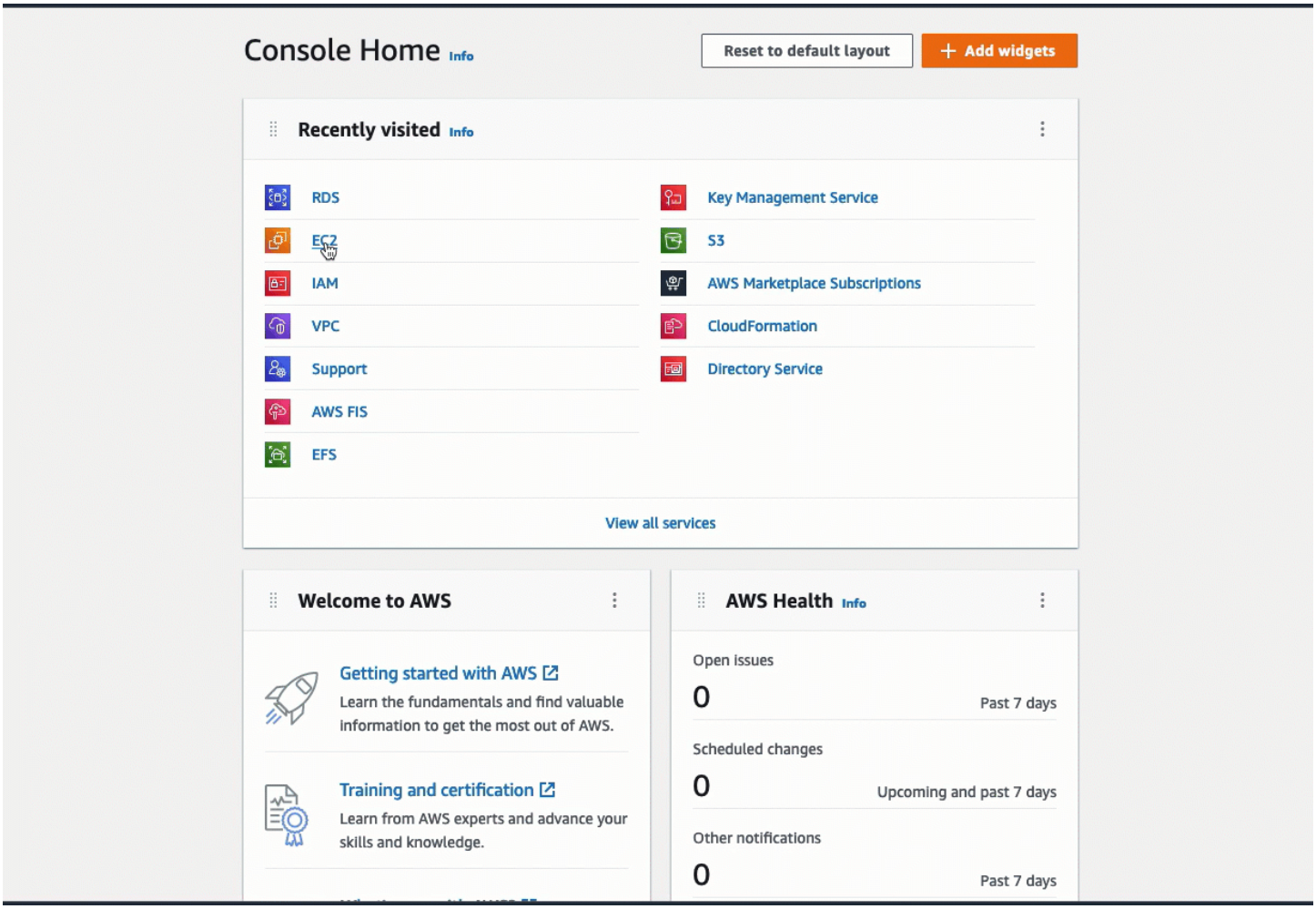
- Descripción: regla para permitir conexiones a **`database-tutorial`** desde cualquier instancia a la que esté adjunto este grupo de seguridad

8. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
9. En el panel de navegación, elija Databases (Bases de datos).
10. Elija la base de datos de RDS que creó para este tutorial.
11. En la pestaña Connectivity & security (Conectividad y seguridad), en Security (Seguridad), VPC security groups (Grupos de seguridad de VPC), compruebe que aparezca un grupo de seguridad denominado rds-ec2-***x***.
12. Elija el grupo de seguridad rds-ec2-***x***. Se abre la pantalla Security Groups (Grupos de seguridad) de la consola de EC2.
13. Elija el grupo de seguridad rds-ec2-***x*** para abrirlo.
14. Elija la pestaña Reglas de entrada.
15. Compruebe que exista la siguiente regla de grupo de seguridad, como se muestra a continuación:

    - Tipo: MySQL/Aurora
    - Intervalo de puertos: 3306
    - Origen: ***sg-0987654321example***/ec2-rds-***x***. Este es el grupo de seguridad que se asigna a la instancia de EC2 que comprobó en los pasos anteriores.
    - Descripción: Rule to allow connections from EC2 instances with ***sg-1234567890example*** attached (Regla para permitir conexiones desde instancias de EC2 con sg-1234567890example adjunto)

    Al comprobar que estos grupos de seguridad y reglas de grupos de seguridad existen y están asignados a la instancia de EC2 y a la base de datos de RDS tal como se describe en este procedimiento, puede comprobar que la conexión se configuró automáticamente mediante la característica de conexión automática.

Ver animación: comprobación de la configuración de la conexión



Completó la opción 2 de este tutorial. Ahora puede completar la opción 3, que le enseña cómo configurar manualmente los grupos de seguridad que se crearon automáticamente en la opción 2.

Opción 3: conexión manual de la instancia de EC2 a la base de datos de RDS imitando la característica de conexión automática

Objetivo

El objetivo de la opción 3 es aprender a configurar manualmente la conexión entre una instancia de EC2 y una base de datos de RDS a partir de la reproducción manual de la configuración de la característica de conexión automática.

Antes de empezar

Para completar este tutorial, necesitará lo siguiente:

- Una instancia de EC2 que esté en la misma VPC que la base de datos de RDS. Puede utilizar una instancia de EC2 existente o seguir los pasos de la tarea 1 para crear una instancia nueva.
- Una base de datos de RDS que esté en la misma VPC que la instancia de EC2. Puede utilizar una base de datos de RDS existente o seguir los pasos de la tarea 2 para crear una base de datos nueva.
- Permisos para llamar a las siguientes operaciones. Si completó la opción 1 de este tutorial, ya tiene estos permisos.
  - `ec2:AssociateRouteTable`
  - `ec2:AuthorizeSecurityGroupEgress`
  - `ec2:CreateRouteTable`
  - `ec2:CreateSecurityGroup`
  - `ec2:CreateSubnet`
  - `ec2:DescribeInstances`
  - `ec2:DescribeNetworkInterfaces`
  - `ec2:DescribeRouteTables`
  - `ec2:DescribeSecurityGroups`
  - `ec2:DescribeSubnets`
  - `ec2:ModifyNetworkInterfaceAttribute`
  - `ec2:RevokeSecurityGroupEgress`

Tareas para completar la opción 3

- Tarea 1: inicialización de una instancia de EC2 (opcional)
- Tarea 2: creación de una base de datos de RDS (opcional)
- Tarea 3: conexión manual de la instancia de EC2 a la base de datos de RDS mediante la creación de grupos de seguridad y su asignación a las instancias

Tarea 1: inicialización de una instancia de EC2 (opcional)

> **Note**
>
> El objetivo de este tutorial no es iniciar una instancia. Si ya tiene una instancia de Amazon EC2 y desea utilizarla en este tutorial, puede omitir esta tarea.

Objetivo de la tarea

El objetivo de esta tarea es iniciar una instancia de EC2 para poder completar la tarea 3, en la que se configura la conexión entre la instancia de EC2 y la base de datos de Amazon RDS.

Pasos para iniciar una instancia de EC2

Para este tutorial, siga los pasos que se indican a continuación para iniciar una instancia de EC2.

Para ver una animación de estos pasos, consulte Ver animación: inicialización de una instancia de EC2.

Configuración de instancias de EC2

Los pasos de esta tarea configuran la instancia de EC2 de la siguiente manera:

- Nombre de instancia: **`tutorial-instance`**
- AMI: Amazon Linux 2
- Tipo de instancia: `t2.micro`
- Asignar automáticamente IP pública: habilitado
- Grupo de seguridad con las tres reglas siguientes:
  - Permitir SSH desde su dirección IP
  - Permitir el tráfico HTTPS desde cualquier lugar
  - Permitir el tráfico HTTP desde cualquier lugar

> **Important**
>
> En un entorno de producción, tiene que configurar la instancia para que se ajuste a sus necesidades específicas.

Para iniciar una instancia de EC2

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de EC2, elija Launch Instance (iniciar instancia).
3. En Name and tags (Nombre y etiquetas), ingrese un nombre para identificar la instancia en Name (Nombre). En este tutorial, asigne el nombre **`tutorial-instance-manual-1`** a la

instancia. Si bien el nombre de la instancia no es obligatorio, le ayudará a identificarla más fácilmente.

4. En Application and OS Images (Imágenes de aplicaciones y sistema operativo), elija una AMI que se adapte a las necesidades de su servidor web. En este tutorial, se utiliza Amazon Linux.
5. En Instance type (Tipo de instancia), para Instance type (Tipo de instancia), seleccione uno que se adapte a las necesidades de su servidor web. En este tutorial se utiliza un `t2.micro`.

   > **Note**
   >
   > Puede usar Amazon EC2 con el nivel gratuito siempre que su cuenta de AWS tenga menos de 12 meses de antigüedad y elija un tipo de instancia `t2.micro` (o `t3.micro` en las regiones en las que `t2.micro` no esté disponible).

6. En Key pair (login) (Par de claves [inicio de sesión]), para Key pair name (Nombre del par de claves), elija el par de claves.
7. En Network settings (Configuración de red), haga lo siguiente:

   a. En Network (Red) y Subnet (Subred), si no hizo cambios en la VPC ni las subredes predeterminadas, puede conservar la configuración predeterminada.

      Si hizo cambios en la VPC o las subredes predeterminadas, compruebe lo siguiente:

      i. La instancia debe estar en la misma región que la base de datos de RDS. De forma predeterminada, solo tiene una VPC.

      ii. La VPC en la que va a iniciar la instancia debe tener una puerta de enlace de Internet conectada para que pueda acceder al servidor web desde Internet. La VPC predeterminada se configura automáticamente con una puerta de enlace de Internet.

      iii. Para garantizar que la instancia reciba una dirección IP pública, en Auto-assign public IP (Asignar automáticamente IP pública), compruebe que la opción Enable (Habilitar) esté seleccionada. Si la opción Disable (Deshabilitar) está seleccionada, elija Edit (Editar) (a la derecha de Network Settings [Configuración de red]) y, a continuación, en Auto-assign public IP (Asignar automáticamente IP pública), elija Enable (Habilitar).

   b. Para conectarse a la instancia mediante SSH, necesita una regla de grupo de seguridad que autorice el tráfico SSH (Linux) o RDP (Windows) desde la dirección IPv4 pública del equipo. De forma predeterminada, al iniciar una instancia, se crea un nuevo grupo de seguridad con una regla que permite el tráfico SSH de entrada desde cualquier lugar.

Para asegurarse de que solo su dirección IP pueda conectarse a la instancia, en Firewall (security groups) (Firewall [grupos de seguridad]), en la lista desplegable situada junto a la casilla Allow SSH traffic from (Permitir tráfico SSH desde), seleccione My IP (Mi IP).

c. Para permitir el tráfico de Internet a la instancia, seleccione las siguientes casillas:

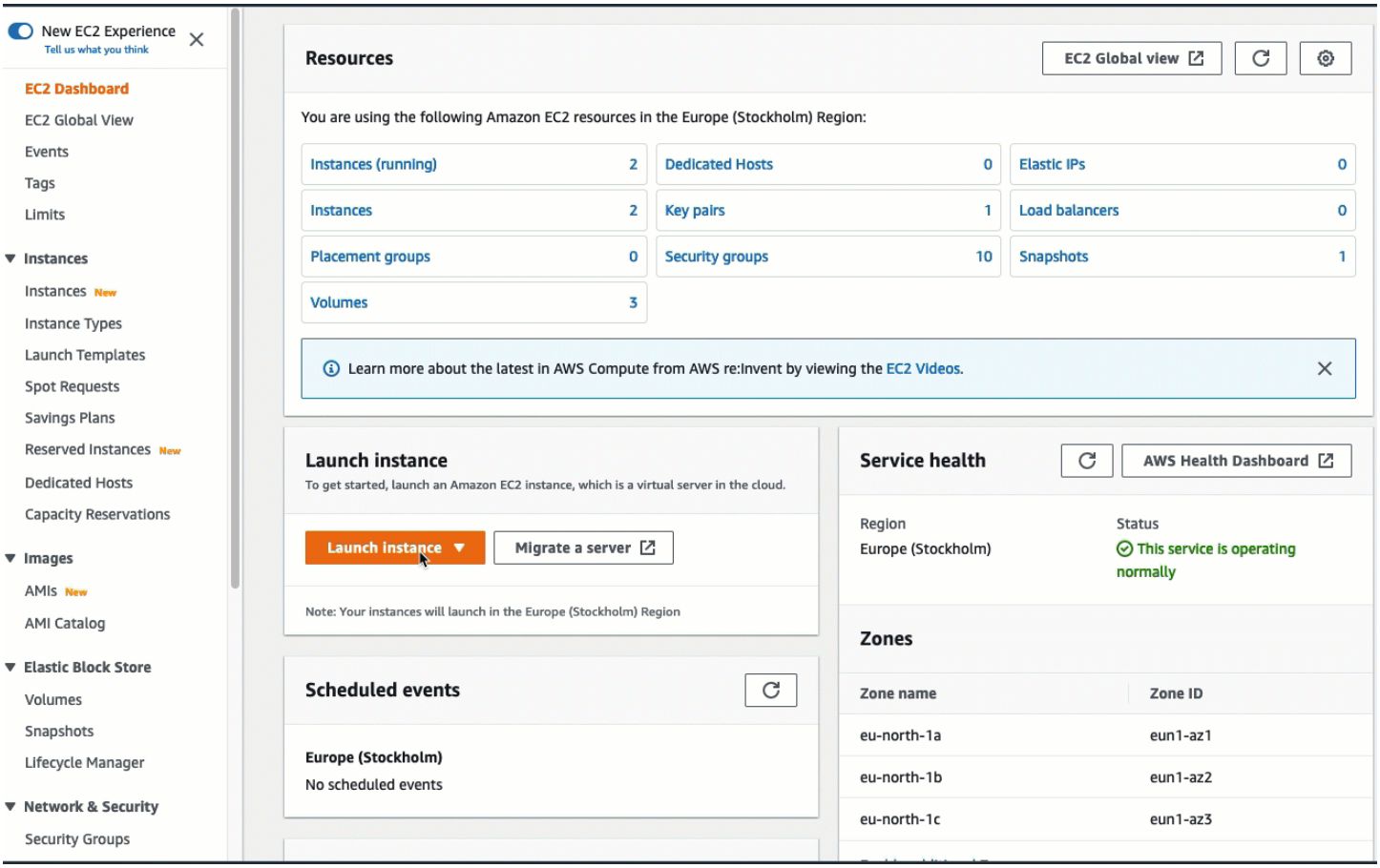
- Allow HTTPs traffic from the internet (Permitir el tráfico HTTPS desde Internet)
- Allow HTTP traffic from the internet (Permitir el tráfico HTTP desde Internet)

8. En el panel Summary (Resumen), revise la configuración de la instancia y, a continuación, elija Launch instance (iniciar instancia).
9. Elija Ver todas las instancias para cerrar la página de confirmación y volver a la consola. El estado inicial de la instancia será `pending` y, a continuación, pasará a `running`.

   Si se produce un error al iniciar la instancia o el estado pasa inmediatamente a `terminated` en lugar de `running`, consulte Solucionar problemas de lanzamiento de instancias.

Para obtener más información acerca de cómo iniciar una instancia, consulte Lance una instancia con el nuevo asistente de inicialización de instancias.

Ver animación: inicialización de una instancia de EC2



Ya tiene todo listo para Tarea 2: creación de una base de datos de RDS (opcional).

Tarea 2: creación de una base de datos de RDS (opcional)

> **Note**
>
> El objetivo de esta parte del tutorial no es crear una base de datos de RDS. Si ya tiene una base de datos de RDS y desea utilizarla en este tutorial, puede omitir esta tarea.

Objetivo de la tarea

El objetivo de esta tarea es crear una base de datos de RDS. Esta instancia se utilizará en la tarea 3 cuando la conecte a la instancia de EC2.

Pasos para crear una base de datos de RDS

Siga los pasos que se indican a continuación para crear una base de datos de RDS para la opción 3 de este tutorial.

Para ver una animación de estos pasos, consulte Ver animación: creación de una instancia de la base de datos.

Configuración de la base de datos de RDS

Los pasos de esta tarea configuran la base de datos de RDS de la siguiente manera:

- Tipo de motor: MySQL
- Plantilla: nivel gratuito
- Identificador de la instancia de la base de datos: **`tutorial-database-manual`**
- Clase de instancia de la base de datos: `db.t3.micro`

> **Important**
>
> En un entorno de producción, tiene que configurar la instancia para que se ajuste a sus necesidades específicas.

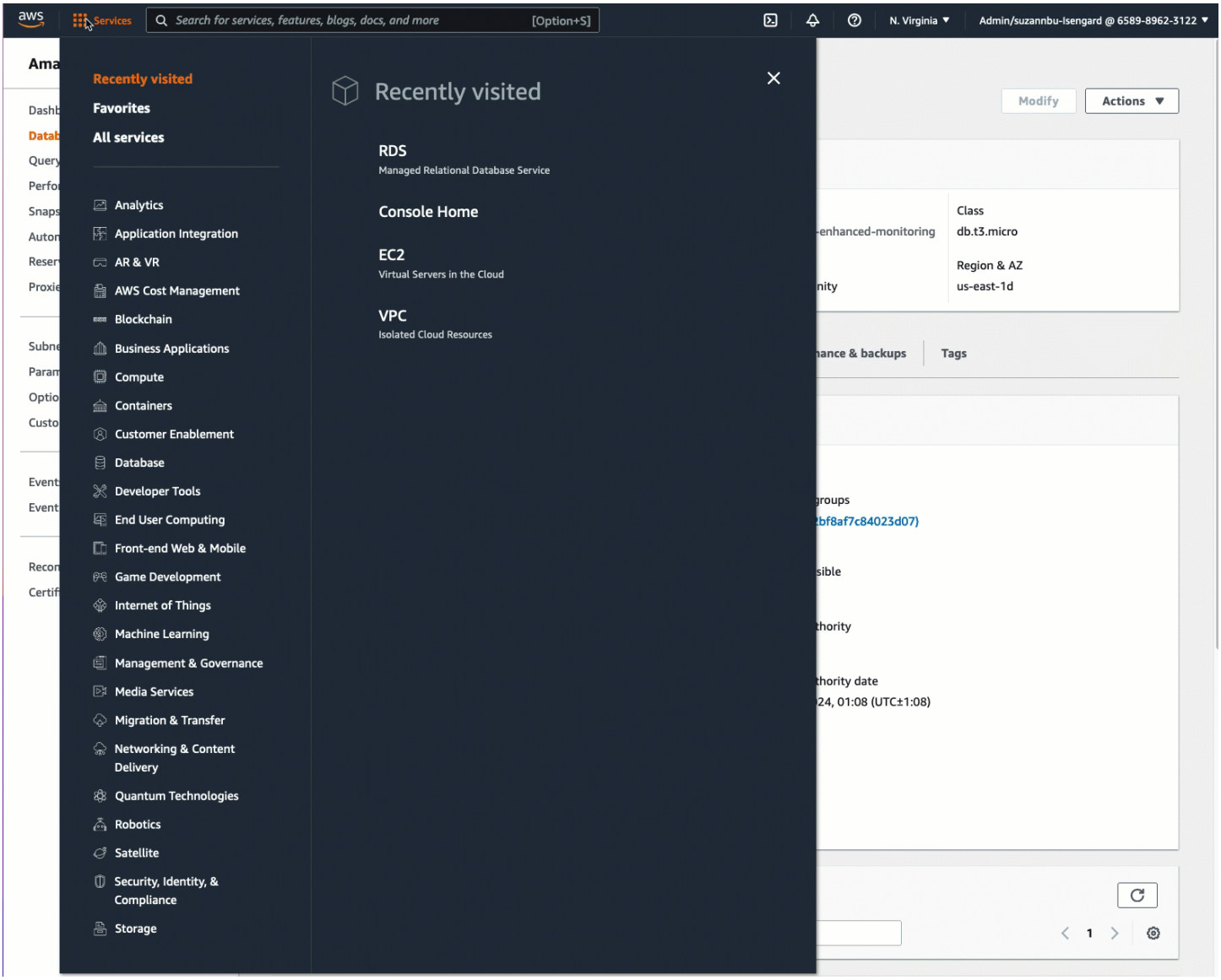
Para crear una instancia de la base de datos MySQL

1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el selector de regiones (en la parte superior derecha), elija la Región de AWS en la que creó la instancia de EC2. La instancia de EC2 y la instancia de la base de datos deben estar en la misma región.
3. En el panel, elija Create database (Crear base de datos).
4. En Choose a database creation method (Elegir un método de creación de base de datos), elija Easy create (Creación sencilla). Al elegir esta opción, no está disponible la característica de conexión automática para configurar automáticamente la conexión.
5. En Engine options (Opciones del motor), para Engine type (Tipo de motor), elija MySQL.
6. En DB instance size (Tamaño de la instancia de la base de datos), seleccione Free tier (Capa gratuita).

7. En DB instance identifier (Identificador de instancias de bases de datos), ingrese un nombre para la base de datos de RDS. En este tutorial, escriba **`tutorial-database-manual`**.
8. En Master username (Nombre de usuario maestro), deje el nombre predeterminado, que es **`admin`**.
9. En Master password (Contraseña maestra), ingrese una contraseña que pueda recordar para este tutorial y, a continuación, en Confirm password (Confirmar contraseña), vuelva a escribirla.
10. Elija Crear base de datos.

    En la pantalla Databases (Bases de datos), Status (Estado) de la nueva instancia de la base de datos es Creating (En creación) hasta que la instancia de la base de datos esté lista para usarse. Cuando el estado cambie a Available (Disponible), podrá conectarse a la instancia de la base de datos. Dependiendo de la clase de instancia de la base de datos y de la cantidad de almacenamiento, es posible que la nueva instancia tarde hasta 20 minutos en estar disponible.

Ver animación: creación de una instancia de la base de datos



Ya tiene todo listo para [Tarea 3: conexión manual de la instancia de EC2 a la base de datos de RDS mediante la creación de grupos de seguridad y su asignación a las instancias](#).

Tarea 3: conexión manual de la instancia de EC2 a la base de datos de RDS mediante la creación de grupos de seguridad y su asignación a las instancias

Objetivo de la tarea

El objetivo de esta tarea es reproducir la configuración de conexión de la característica de conexión automática mediante el siguiente proceso manual: se crean dos grupos de seguridad nuevos y, a continuación, se agrega uno de los grupos de seguridad a la instancia de EC2 y el otro, a la base de datos de RDS.

Pasos para crear nuevos grupos de seguridad y agregarlos a las instancias

Siga los pasos que se indican a continuación para conectar una instancia de EC2 a la base de datos de RDS mediante la creación de dos grupos de seguridad nuevos. A continuación, agregue uno de los grupos de seguridad a la instancia de EC2 y el otro, a la base de datos de RDS.

Para crear dos grupos de seguridad nuevos y asignar uno a la instancia de EC2 y el otro, a la base de datos de RDS

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. Primero cree el grupo de seguridad que va a agregar a la instancia de EC2, como se muestra a continuación:
    a. En el panel de navegación, seleccione Grupos de seguridad.
    b. Seleccione Crear grupo de seguridad.
    c. En Security group name (Nombre del grupo de seguridad), escriba un nombre descriptivo para el grupo de seguridad. En este tutorial, escriba **`ec2-rds-manual-configuration`**.
    d. En Description (Descripción), ingrese una breve descripción. En este tutorial, escriba **`EC2 instance security group to allow EC2 instance to securely connect to RDS database`**.
    e. Elija Crear grupo de seguridad. Volverá a este grupo de seguridad para agregar una regla de salida después de crear el grupo de seguridad de la base de datos de RDS.
3. Ahora, cree el grupo de seguridad para agregarlo a la base de datos de RDS, como se muestra a continuación:
    a. En el panel de navegación, elija Security Groups.
    b. Seleccione Crear grupo de seguridad.
    c. En Security group name (Nombre del grupo de seguridad), escriba un nombre descriptivo para el grupo de seguridad. En este tutorial, escriba **`rds-ec2-manual-configuration`**.
    d. En Description (Descripción), ingrese una breve descripción. En este tutorial, escriba **`RDS database security group to allow EC2 instance to securely connect to RDS database`**.
    e. En Inbound rules (Reglas de entrada), elija Add Rule (Agregar regla) y haga lo siguiente:
        i. En Type (Tipo), elija MySQL/Aurora.

ii. En Source (Origen), elija el grupo de seguridad de la instancia de EC2 ec2-rds-manual-configuration que creó en el paso 2 de este procedimiento.

f. Elija Crear grupo de seguridad.

4. Edite el grupo de seguridad de la instancia de EC2 para agregar una regla de salida, como se muestra a continuación:

a. En el panel de navegación, elija Security Groups.

b. Seleccione el grupo de seguridad de instancias de EC2 (que nombró como **`ec2-rds-manual-configuration`**) y elija la pestaña Outbound rules (Reglas de salida).

c. Elija Edit outbound rules (Editar reglas de salida).

d. Elija Add Rule (Agregar regla) y haga lo siguiente:

i. En Type (Tipo), elija MySQL/Aurora.

ii. En Source (Origen), elija el grupo de seguridad de la base de datos de RDS rds-ec2-manual-configuration que creó en el paso 3 de este procedimiento.

iii. Seleccione Guardar reglas.

5. Agregue el grupo de seguridad de instancias de EC2 a la instancia de EC2, como se muestra a continuación:

a. En el panel de navegación, seleccione Instances (Instancia[s]).

b. Seleccione la instancia de EC2 y elija Actions (Acciones), Security (Seguridad), Change security groups (Cambiar grupos de seguridad).

c. En Associated security groups (Grupos de seguridad asociados), elija el campo Select security groups (Seleccionar grupos de seguridad), elija ec2-rds-manual-configuration que creó anteriormente y, a continuación, elija Add security group (Agregar grupo de seguridad).

d. Seleccione Guardar.

6. Agregue el grupo de seguridad de bases de datos de RDS a la base de datos de RDS, como se muestra a continuación:

a. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.

b. En el panel de navegación, elija Databases (Bases de datos) y seleccione la base de datos.

c. Elija Modificar.

d. En Connectivity (Conectividad), en Security group (Grupo de seguridad), elija rds-ec2-manual-configuration que creó anteriormente y, a continuación, elija Continue (Continuar).

e. En Scheduling of modifications (Programación de modificaciones), elija Apply immediately (Aplicar inmediatamente).

f. Elija Modify DB instance (Modificar la instancia de la base de datos).

Ya completó los pasos manuales que imitan los pasos automáticos que se producen cuando utiliza la característica de conexión automática.

Completó la opción 3 de este tutorial. Si completó las opciones 1, 2 y 3 y ya no necesita los recursos que se crearon en este tutorial, debería eliminarlos para evitar incurrir en gastos innecesarios. Para obtener más información, consulte Limpieza.

Limpieza

Ahora que completó el tutorial, se recomienda limpiar (eliminar) todos los recursos que ya no desee utilizar. Limpiar los recursos de AWS evita que la cuenta incurra en cargos adicionales.

Temas

- Terminación de la instancia de EC2
- Eliminación de la base de datos de RDS

Terminación de la instancia de EC2

Si lanzó una instancia de EC2 específicamente para este tutorial, puede cancelarla para dejar de incurrir en los cargos asociados a ella.

Para terminar una instancia mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Seleccione la instancia que creó para este tutorial y elija Instance state (Estado de instancia), Terminate instance (Terminar instancia).
4. Cuando se le indique que confirme, elija Terminar.

Eliminación de la base de datos de RDS

Si creó una base de datos de RDS específicamente para este tutorial, puede eliminarla para dejar de incurrir en los cargos asociados a ella.

Para eliminar una base de datos de RDS mediante la consola

1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos).
3. Seleccione la base de datos de RDS que creó para este tutorial y elija Actions (Acciones), Delete (Eliminar).
4. Escriba **`delete me`** en el cuadro y, a continuación, elija Delete (Eliminar).

Identificación de instancias EC2

Es posible que tenga que determinar si su aplicación se ejecuta en una instancia EC2, específicamente si tiene un entorno de computación combinado. Cada instancia tiene un documento de identidad de instancia firmado que puede comprobar criptográficamente. Puede encontrar estos documentos en la siguiente dirección local no enrutable `http://169.254.169.254/latest/dynamic/instance-identity/`. Para obtener más información, consulte Documentos de identidad de instancias.

Revise el UUID del sistema

Puede obtener el UUID del sistema y buscarlo en el octeto inicial del UUID para `EC2` (en Linux, puede estar en minúsculas `ec2`). Este método es rápido, pero potencialmente impreciso, ya que existe una pequeña posibilidad de que un sistema que no es una instancia EC2 tenga un UUID que comience con estos caracteres. Además, algunas versiones de SMBIOS utilizan el formato little-endian, que no incluye `EC2` al principio del UUID. Este podría ser el caso de las instancias EC2 que utilizan SMBIOS 2.4 para Windows o de distribuciones de Linux distintas de Amazon Linux 2 que tienen su propia implementación de SMBIOS.

Ejemplo de Linux: obtención del UUID de DMI (solo AMI HVM)

Utilice el siguiente comando para obtener el UUID mediante la Interfaz de administración de escritorio (DMI):

```
[ec2-user ~]$ sudo dmidecode --string system-uuid
```

En el siguiente ejemplo de resultado, el UUID comienza por "EC2", lo que indica que el sistema es probablemente una instancia de EC2.

```
EC2E1916-9099-7CAF-FD21-012345ABCDEF
```

En la siguiente salida de ejemplo, el UUID se representa en formato little-endian.

```
45E12AEC-DCD1-B213-94ED-012345ABCDEF
```

Otra opción para instancias integradas en el sistema Nitro, es usar el siguiente comando:

```
[ec2-user ~]$ cat /sys/devices/virtual/dmi/id/board_asset_tag
```

Si la salida es un ID de instancia, como la siguiente salida de ejemplo, el sistema es una instancia de EC2:

```
i-0af01c0123456789a
```

Ejemplo de Linux: obtención del UUID del hipervisor (solo AMI PV)

Utilice el siguiente comando para obtener el UUID del hipervisor:

```
[ec2-user ~]$ cat /sys/hypervisor/uuid
```

En el siguiente ejemplo de resultado, el UUID comienza por "ec2", lo que indica que el sistema es probablemente una instancia de EC2.

```
ec2e1916-9099-7caf-fd21-012345abcdef
```

Ejemplo de Windows: obtención del UUID con WMI o Windows PowerShell

Use la línea de comando Windows Management Instrumentation Command (WMIC) del modo siguiente:

```
wmic path win32_computersystemproduct get uuid
```

Si utiliza Windows PowerShell, use el cmdlet Get-WmiObject del modo siguiente:

```
PS C:\> Get-WmiObject -query "select uuid from Win32_ComputerSystemProduct" | Select
 UUID
```

En el siguiente ejemplo de resultado, el UUID comienza por "EC2", lo que indica que el sistema es probablemente una instancia de EC2.

```
EC2AE145-D1DC-13B2-94ED-012345ABCDEF
```

En las instancias que usan SMBIOS 2.4, se puede representar el UUID en formato little-endian, por ejemplo:

```
45E12AEC-DCD1-B213-94ED-012345ABCDEF
```

Examine el identificador de generación de máquinas virtuales del sistema

Un identificador de generación de máquinas virtuales consiste en un búfer único de 128 bits que se interpreta como un identificador criptográfico aleatorio de números enteros. Puede recuperar el identificador de generación de máquinas virtuales para identificar su instancia de Amazon Elastic Compute Cloud (EC2). El identificador de generación se encuentra expuesto dentro del sistema operativo invitado de la instancia a través de una entrada de la tabla ACPI. El valor cambiará si el equipo se clona, copia o importa en AWS, como por ejemplo con VM Import/Export.

Ejemplo: Recupere el identificador de generación de máquinas virtuales de Linux

Puede utilizar los siguientes comandos para recuperar el identificador de generación de máquinas virtuales de sus instancias que ejecutan Linux.

Amazon Linux 2

1. Actualice sus paquetes de software existentes, según sea necesario, mediante el siguiente comando:

   ```
   sudo yum update
   ```

2. Si es necesario, obtenga el paquete busybox con el siguiente comando:

   ```
   sudo curl https://www.rpmfind.net/linux/epel/next/8/Everything/x86_64/Packages/
   b/busybox-1.35.0-2.el8.next.x86_64.rpm --output busybox.rpm
   ```

3. Si es necesario, instale los paquetes de requisitos previos mediante el siguiente comando:

   ```
   sudo yum install busybox.rpm iasl -y
   ```

4. Ejecute el siguiente comando `iasl` para obtener la salida de la tabla ACPI:

```
sudo iasl -p ./SSDT2 -d /sys/firmware/acpi/tables/SSDT2
```

5. Ejecute el siguiente comando para revisar la salida del comando `iasl`:

```
cat SSDT2.dsl
```

La salida debería proporcionar el espacio de direcciones necesario para recuperar el identificador de generación de máquinas virtuales:

```
Intel ACPI Component Architecture
ASL+ Optimizing Compiler/Disassembler version 20190509
Copyright (c) 2000 - 2019 Intel Corporation

File appears to be binary: found 32 non-ASCII characters, disassembling
Binary file appears to be a valid ACPI table, disassembling
Input file /sys/firmware/acpi/tables/SSDT2, Length 0x7B (123) bytes
ACPI: SSDT 0x0000000000000000 00007B (v01 AMAZON AMZNSSDT 00000001 AMZN
 00000001)
Pass 1 parse of [SSDT]
Pass 2 parse of [SSDT]
Parsing Deferred Opcodes (Methods/Buffers/Packages/Regions)

Parsing completed
Disassembly completed
ASL Output:    ./SSDT2.dsl - 1065 bytes
$
/*
* Intel ACPI Component Architecture
* AML/ASL+ Disassembler version 20190509 (64-bit version)
* Copyright (c) 2000 - 2019 Intel Corporation
*
* Disassembling to symbolic ASL+ operators
*
* Disassembly of /sys/firmware/acpi/tables/SSDT2, Tue Mar 29 16:15:14 2022
*
* Original Table Header:
*     Signature        "SSDT"
*     Length           0x0000007B (123)
*     Revision         0x01
*     Checksum         0xB8
```

```
*     OEM ID           "AMAZON"
*     OEM Table ID     "AMZNSSDT"
*     OEM Revision     0x00000001 (1)
*     Compiler ID      "AMZN"
*     Compiler Version 0x00000001 (1)
*/
DefinitionBlock ("", "SSDT", 1, "AMAZON", "AMZNSSDT", 0x00000001)
{
Scope (\_SB)
{
    Device (VMGN)
    {
        Name (_CID, "VM_Gen_Counter")  // _CID: Compatible ID
        Name (_DDN, "VM_Gen_Counter")  // _DDN: DOS Device Name
        Name (_HID, "AMZN0000")  // _HID: Hardware ID
        Name (ADDR, Package (0x02)
        {
            0xFED01000,
            Zero
        })
    }
}
}
```

6. (Opcional) Aumente los permisos del terminal para los pasos restantes con el siguiente comando:

```
sudo -s
```

7. Utilice el siguiente comando para almacenar el espacio de direcciones recopilado previamente:

```
VMGN_ADDR=0xFED01000
```

8. Utilice el siguiente comando para iterar a través del espacio de direcciones y crear el identificador de generación de máquinas virtuales:

```
for offset in 0x0 0x4 0x8 0xc; do busybox devmem $(($VMGN_ADDR + $offset)) | sed
 's/0x//' | sed -z '$ s/\n$//' >> vmgenid; done
```

9. Recupere el identificador de generación de máquinas virtuales del archivo de salida con el siguiente comando:

```
cat vmgenid ; echo
```

El resultado debería ser similar al siguiente:

```
EC2F335D979132C4165896753E72BD1C
```

Ubuntu

1. Actualice sus paquetes de software existentes, según sea necesario, mediante el siguiente comando:

```
sudo apt update
```

2. Si es necesario, instale los paquetes de requisitos previos mediante el siguiente comando:

```
sudo apt install busybox iasl -y
```

3. Ejecute el siguiente comando `iasl` para obtener la salida de la tabla ACPI:

```
sudo iasl -p ./SSDT2 -d /sys/firmware/acpi/tables/SSDT2
```

4. Ejecute el siguiente comando para revisar la salida del comando `iasl`:

```
cat SSDT2.dsl
```

La salida debería proporcionar el espacio de direcciones necesario para recuperar el identificador de generación de máquinas virtuales:

```
Intel ACPI Component Architecture
ASL+ Optimizing Compiler/Disassembler version 20190509
Copyright (c) 2000 - 2019 Intel Corporation

File appears to be binary: found 32 non-ASCII characters, disassembling
Binary file appears to be a valid ACPI table, disassembling
Input file /sys/firmware/acpi/tables/SSDT2, Length 0x7B (123) bytes
ACPI: SSDT 0x0000000000000000 00007B (v01 AMAZON AMZNSSDT 00000001 AMZN
 00000001)
Pass 1 parse of [SSDT]
Pass 2 parse of [SSDT]
```

```
Parsing Deferred Opcodes (Methods/Buffers/Packages/Regions)

Parsing completed
Disassembly completed
ASL Output:    ./SSDT2.dsl - 1065 bytes
$
/*
* Intel ACPI Component Architecture
* AML/ASL+ Disassembler version 20190509 (64-bit version)
* Copyright (c) 2000 - 2019 Intel Corporation
*
* Disassembling to symbolic ASL+ operators
*
* Disassembly of /sys/firmware/acpi/tables/SSDT2, Tue Mar 29 16:15:14 2022
*
* Original Table Header:
*     Signature        "SSDT"
*     Length           0x0000007B (123)
*     Revision         0x01
*     Checksum         0xB8
*     OEM ID           "AMAZON"
*     OEM Table ID     "AMZNSSDT"
*     OEM Revision     0x00000001 (1)
*     Compiler ID      "AMZN"
*     Compiler Version 0x00000001 (1)
*/
DefinitionBlock ("", "SSDT", 1, "AMAZON", "AMZNSSDT", 0x00000001)
{
Scope (\_SB)
{
    Device (VMGN)
    {
        Name (_CID, "VM_Gen_Counter")  // _CID: Compatible ID
        Name (_DDN, "VM_Gen_Counter")  // _DDN: DOS Device Name
        Name (_HID, "AMZN0000")  // _HID: Hardware ID
        Name (ADDR, Package (0x02)
        {
            0xFED01000,
            Zero
        })
    }
}
}
```

5. (Opcional) Aumente los permisos del terminal para los pasos restantes con el siguiente comando:

```
sudo -s
```

6. Utilice los siguientes comandos para almacenar el espacio de direcciones recopilado previamente:

```
VMGN_ADDR=0xFED01000
```

7. Utilice el siguiente comando para iterar a través del espacio de direcciones y crear el identificador de generación de máquinas virtuales:

```
for offset in 0x0 0x4 0x8 0xc; do busybox devmem $(($VMGN_ADDR + $offset)) | sed
 's/0x//' | sed -z '$ s/\n$//' >> vmgenid; done
```

8. Recupere el identificador de generación de máquinas virtuales del archivo de salida con el siguiente comando:

```
cat vmgenid ; echo
```

   El resultado debería ser similar al siguiente:

```
EC2F335D979132C4165896753E72BD1C
```

Ejemplo: Recupere el identificador de generación de máquinas virtuales de Windows

Puede crear una aplicación de ejemplo para recuperar el identificador de generación de máquinas virtuales de las instancias que ejecutan Windows. Para obtener más información, consulte Obtención del identificador de generación de máquinas virtuales en la documentación de Microsoft.

Administración de la configuración del sistema para su instancia de Amazon EC2

Una vez inicializada la instancia, puede iniciar sesión como administrador para realizar cambios. Esta sección se centra en la administración de la configuración del sistema para su instancia.

Contenido

Establezca el tiempo de su instancia de Amazon EC2.

Una referencia horaria coherente y precisa en su instancia de Amazon EC2 resulta crucial para muchas tareas y procesos del servidor. Las marcas de tiempo en los registros del sistema desempeñan un papel esencial a la hora de identificar cuándo se produjeron los problemas y el orden cronológico de los eventos. Cuando use la AWS CLI o un SDK de AWS para realizar solicitudes desde la instancia, estas herramientas firman las solicitudes en su nombre. Si la configuración de fecha y hora de la instancia no es correcta, podría producirse una discrepancia entre la fecha de la firma y la fecha de la solicitud y AWS rechazaría las solicitudes.

Para abordar este importante aspecto, Amazon ofrece el Servicio de sincronización temporal de Amazon, que está disponible desde todas las instancias de EC2 y que utilizan varios Servicios de AWS. El servicio utiliza una flota de relojes atómicos de referencia conectados vía satélite en cada Región de AWS para entregar lecturas horarias precisas y actuales del estándar global de la hora universal coordinada (UTC).

El Servicio de sincronización temporal de Amazon utiliza el protocolo de tiempo de redes (NTP) o proporciona un reloj de hardware local del protocolo de tiempo de precisión (PTP) en las instancias compatibles. El reloj de hardware de PTP admite una conexión NTP o una conexión PTP directa. La conexión NTP y la conexión PTP directa utilizan el mismo origen horaria de alta precisión, pero la conexión PTP directa es más precisa que la conexión NTP. La conexión NTP al Servicio de sincronización temporal de Amazon admite la difuminación temporal, mientras que la conexión PTP al reloj de hardware de PTP no extiende la hora. Para obtener más información, consulte Segundos intercalares.

Para lograr un rendimiento óptimo, le recomendamos que use el Servicio de sincronización temporal de Amazon en sus instancias EC2. Para hacer una copia de seguridad del Servicio de sincronización

temporal de Amazon local en sus instancias y conectar recursos ajenos a Amazon EC2 al Servicio de sincronización temporal de Amazon, puede utilizar el Servicio de sincronización temporal de Amazon público que se encuentra en `time.aws.com`. El Servicio de sincronización temporal de Amazon público, igual que el Servicio de sincronización temporal de Amazon local, difumina automáticamente los segundos intercalares que se agregan a la hora UTC. El Servicio de sincronización temporal de Amazon público es compatible en todo el mundo con nuestra flota de relojes atómicos de referencia conectados vía satélite en cada Región de AWS.

Temas

Configuración de una instancia para que use el Servicio de sincronización temporal de Amazon local

Sus instancias pueden acceder al Servicio de sincronización temporal de Amazon local de la siguiente manera:

- A través de NTP en los siguientes puntos de conexión de direcciones IP:
  - IPv4: `169.254.169.123`
  - IPv6: `fd00:ec2::123` (solo se puede acceder a través de las instancias integradas en el AWS Nitro System.)
- (Solo Linux) A través de una conexión PTP directa para conectarse a un reloj de hardware de PTP local:
  - `PHC0`

Las AMI de Amazon Linux, las AMI de Windows y la mayoría de las AMI de socios configuran la instancia para que utilice el punto de conexión IPv4 NTP de forma predeterminada. Esta es la configuración recomendada para la mayoría de las cargas de trabajo de clientes. No se requiere

ninguna configuración adicional para las instancias iniciadas desde estas AMI, a menos que desee utilizar el punto de conexión IPv6 o conectarse directamente al reloj de hardware de PTP.

Las conexiones NTP y PTP no requieren ningún cambio en la configuración de la VPC y la instancia no requiere acceso a Internet.

> **Note**
>
> Solo las instancias de Linux pueden utilizar una conexión PTP directa para conectarse a un reloj de hardware de PTP local. Las instancias de Windows utilizan NTP para conectarse al reloj de hardware de PTP local.

Temas

Conexión al punto de conexión de IPv4 del Servicio de sincronización temporal de Amazon

En esta sección se describe cómo configurar su instancia de modo que use el Servicio de sincronización temporal de Amazon local a través del punto de conexión IPv4.

Consulte las instrucciones del sistema operativo de su instancia.

Linux

AL2023 y las últimas versiones de las AMI de Amazon Linux 2 y Amazon Linux se configuran para utilizar el punto de conexión IPv4 del Servicio de sincronización temporal de Amazon de forma predeterminada. No se requiere ninguna configuración adicional para las instancias iniciadas desde estas AMI y puede omitir los siguientes procedimientos.

Si utiliza una AMI que no tiene el Servicio de sincronización temporal de Amazon configurado de forma predeterminada, utilice uno de los siguientes procedimientos para configurar el Servicio de sincronización temporal de Amazon en su instancia mediante el cliente `chrony`. Es necesario agregar una entrada de servidor para el Servicio de sincronización temporal de Amazon al archivo de configuración `chrony`.

Consulte las instrucciones del sistema operativo de su instancia.

Amazon Linux

Conexión al punto de conexión IPv4 del Servicio de sincronización temporal de Amazon en Amazon Linux mediante chrony

1. Conéctese a su instancia y desinstale el servicio NTP.

```
[ec2-user ~]$ sudo yum erase 'ntp*'
```

2. Instale el paquete `chrony`.

```
[ec2-user ~]$ sudo yum install chrony
```

3. Abra el archivo `/etc/chrony.conf` con cualquier editor de texto (como vim o nano). Verifique que el archivo incluya la siguiente línea:

```
server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
```

   Si la línea existe, el Servicio de sincronización temporal de Amazon ya está configurado para usar el punto de conexión IPv4 del Servicio de sincronización temporal de Amazon y puede continuar con el siguiente paso. Si no, añada la línea después de cualquier otra instrucción `server` o `pool` que ya se encuentre en el archivo y guarde los cambios.

4. Reinicie daemon `chrony` (`chronyd`).

```
[ec2-user ~]$ sudo service chronyd restart
```

```
Starting chronyd:                                          [  OK  ]
```

> **Note**
>
> En RHEL y CentOS (hasta la versión 6), el nombre del servicio es `chrony` en lugar de `chronyd`.

5. Para configurar que `chronyd` se inicie cada vez que arranque el sistema, utilice el comando `chkconfig`.

```
[ec2-user ~]$ sudo chkconfig chronyd on
```

6. Verifique que `chrony` esté usando el punto de conexión IPv4 `169.254.169.123` para sincronizar la hora.

```
[ec2-user ~]$ chronyc sources -v
```

```
210 Number of sources = 7

  .-- Source mode  '^' = server, '=' = peer, '#' = local clock.
 / .- Source state '*' = current synced, '+' = combined , '-' = not
combined,
| /   '?' = unreachable, 'x' = time may be in error, '~' = time too
variable.
||                                                 .- xxxx [ yyyy ] +/-
zzzz
||      Reachability register (octal) -.           |  xxxx = adjusted
offset,
||      Log2(Polling interval) --.      |          |  yyyy = measured
offset,
||                                \     |          |  zzzz = estimated
error.
||                                 |    |           \
MS Name/IP address         Stratum Poll Reach LastRx Last sample


===============================================================================
^* 169.254.169.123               3   6    17    43    -30us[ -226us] +/-
 287us
^- ec2-12-34-231-12.eu-west>     2   6    17    43   -388us[ -388us] +/-
  11ms
^- tshirt.heanet.ie              1   6    17    44   +178us[  +25us] +/-
1959us
^? tbag.heanet.ie                0   6     0     -     +0ns[   +0ns] +/-
   0ns
^? bray.walcz.net                0   6     0     -     +0ns[   +0ns] +/-
   0ns
^? 2a05:d018:c43:e312:ce77:>     0   6     0     -     +0ns[   +0ns] +/-
   0ns
^? 2a05:d018:dab:2701:b70:b>     0   6     0     -     +0ns[   +0ns] +/-
   0ns
```

En la respuesta obtenida, `^*` indica el origen de hora preferido.

7. Verifique que `chrony` muestre las métricas de sincronización de hora.

```
[ec2-user ~]$ chronyc tracking
```

```
Reference ID    : A9FEA97B (169.254.169.123)
        Stratum         : 4
        Ref time (UTC)  : Wed Nov 22 13:18:34 2017
        System time     : 0.000000626 seconds slow of NTP time
        Last offset     : +0.002852759 seconds
        RMS offset      : 0.002852759 seconds
        Frequency       : 1.187 ppm fast
        Residual freq   : +0.020 ppm
        Skew            : 24.388 ppm
        Root delay      : 0.000504752 seconds
        Root dispersion : 0.001112565 seconds
        Update interval : 64.4 seconds
        Leap status     : Normal
```

Ubuntu

Conexión al punto de conexión IPv4 del Servicio de sincronización temporal de Amazon en Ubuntu mediante chrony

1. Conecte su instancia y use `apt` para instalar el paquete `chrony`.

```
ubuntu:~$ sudo apt install chrony
```

> **Note**
>
> De ser necesario, ejecute primero para actualizar su instancia `sudo apt update`.

2. Abra el archivo `/etc/chrony/chrony.conf` con cualquier editor de texto (como vim o nano). Añada la siguiente línea antes de cualquier otra instrucción `server` o `pool` que ya se encuentre en el archivo y guarde los cambios:

```
server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
```

3. Reinicie el servicio `chrony`.

```
ubuntu:~$ sudo /etc/init.d/chrony restart
```

```
Restarting chrony (via systemctl): chrony.service.
```

4. Verifique que `chrony` esté usando el punto de conexión IPv4 `169.254.169.123` para sincronizar la hora.

```
ubuntu:~$ chronyc sources -v
```

```
210 Number of sources = 7

             .-- Source mode  '^' = server, '=' = peer, '#' = local clock.
            / .- Source state '*' = current synced, '+' = combined , '-' = not
 combined,
           | /   '?' = unreachable, 'x' = time may be in error, '~' = time too
 variable.
           ||                                                .- xxxx [ yyyy ]
 +/- zzzz
           ||      Reachability register (octal) -.          |  xxxx =
 adjusted offset,
           ||      Log2(Polling interval) --.      |         |  yyyy =
 measured offset,
           ||                                \     |         |  zzzz =
 estimated error.
           ||                                 |    |          \
           MS Name/IP address         Stratum Poll Reach LastRx Last sample

 ===============================================================================
           ^* 169.254.169.123               3   6    17    12    +15us[  +57us]
 +/-  320us
           ^- tbag.heanet.ie                1   6    17    13  -3488us[-3446us]
 +/- 1779us
           ^- ec2-12-34-231-12.eu-west-     2   6    17    13   +893us[ +935us]
 +/- 7710us
           ^? 2a05:d018:c43:e312:ce77:6     0   6     0   10y     +0ns[   +0ns]
 +/-    0ns
           ^? 2a05:d018:d34:9000:d8c6:5     0   6     0   10y     +0ns[   +0ns]
 +/-    0ns
           ^? tshirt.heanet.ie              0   6     0   10y     +0ns[   +0ns]
 +/-    0ns
```

```
            ^? bray.walcz.net               0   6     0   10y     +0ns[   +0ns]
 +/-    0ns
```

En la salida que se devuelve, en la línea que empieza por `^*`, se indica el origen de la hora preferido.

5. Verifique que `chrony` muestre las métricas de sincronización de hora.

```
ubuntu:~$ chronyc tracking
```

```
Reference ID    : 169.254.169.123 (169.254.169.123)
            Stratum         : 4
            Ref time (UTC)  : Wed Nov 29 07:41:57 2017
            System time     : 0.000000011 seconds slow of NTP time
            Last offset     : +0.000041659 seconds
            RMS offset      : 0.000041659 seconds
            Frequency       : 10.141 ppm slow
            Residual freq   : +7.557 ppm
            Skew            : 2.329 ppm
            Root delay      : 0.000544 seconds
            Root dispersion : 0.000631 seconds
            Update interval : 2.0 seconds
            Leap status     : Normal
```

SUSE Linux

A partir de SUSE Linux Enterprise Server 15, `chrony` es la implementación predeterminada de NTP.

Conexión al punto de conexión IPv4 del Servicio de sincronización temporal de Amazon en SUSE Linux mediante chrony

1. Abra el archivo `/etc/chrony.conf` con cualquier editor de texto (como vim o nano).
2. Verifique que el archivo contenga la siguiente línea:

```
server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
```

Si esta línea no existe, añádala.

3. Comente el resto de líneas de servidores o grupos.

4. Abra yaST y habilite el servicio chrony.

Windows

A partir de la versión de agosto de 2018, las AMI de Windows utilizan el Servicio de sincronización temporal de Amazon de forma predeterminada. No se requiere ninguna configuración adicional para las instancias iniciadas desde estas AMI y puede omitir los siguientes procedimientos.

Si utiliza una AMI que no tiene el Servicio de sincronización temporal de Amazon de forma predeterminada, compruebe primero su configuración de NTP actual. Si la instancia ya utiliza el punto de conexión de IPv4 del Servicio de sincronización temporal de Amazon, no es necesario realizar ninguna otra configuración. Si la instancia no utiliza el Servicio de sincronización temporal de Amazon, complete el procedimiento para cambiar el servidor NTP para que utilice el Servicio de sincronización temporal de Amazon.

Para verificar la configuración de NTP

1. Desde la instancia, abra una ventana del símbolo del sistema.
2. Para obtener la configuración de NTP actual, escriba el siguiente comando:

   ```
   w32tm /query /configuration
   ```

   Este comando devuelve los valores de configuración actuales para la instancia de Windows y mostrará si está conectado al Servicio de sincronización temporal de Amazon.
3. (Opcional) Para obtener el estado de la configuración actual, escriba el siguiente comando:

   ```
   w32tm /query /status
   ```

   Este comando devuelve información como la última vez que la instancia se sincronizó con el servidor NTP y el intervalo de sondeo.

Cómo cambiar el servidor NTP de modo que use el Servicio de sincronización temporal de Amazon

1. Desde la ventana del símbolo del sistema, ejecute el siguiente comando:

   ```
   w32tm /config /manualpeerlist:169.254.169.123 /syncfromflags:manual /update
   ```
2. Para comprobar la nueva configuración, use el comando siguiente:

```
w32tm /query /configuration
```

En la salida que devuelve, verifique que `NtpServer` muestra el punto de conexión IPv4 `169.254.169.123`.

Configuración predeterminada de protocolo de tiempo de redes (NTP) para las AMI de Amazon Windows

Generalmente, las imágenes de máquinas de Amazon (AMI) se ajustan a los valores predeterminados de fábrica, salvo en los casos en que se requieren cambios para que funcione en la infraestructura de EC2. Se ha determinado que las siguientes configuraciones funcionan bien en un entorno virtual, así como para mantener cualquier desfase del reloj en un segundo de precisión:

- Intervalo de actualización: controla la frecuencia con la que el servicio de hora ajustará la hora del sistema para que sea exacta. AWS configura el intervalo de actualización para que se produzca una vez cada dos minutos.
- Servidor NTP: a partir de la versión de agosto de 2018, las AMI ahora utilizan de forma predeterminada el Servicio de sincronización temporal de Amazon. Se puede acceder a este servicio de hora desde cualquier Región de AWS en el punto de conexión IPv4 169.254.169.123. Además, el indicador 0x9 muestra que el servicio de hora está actuando como cliente, y que se debe usar `SpecialPollInterval` para determinar con qué frecuencia debe registrarse en el servidor de hora configurado.
- Tipo: “NTP” significa que el servicio actúa como cliente NTP independiente en lugar de actuar como parte de un dominio.
- Habilitado e InputProvider: el servicio de hora está habilitado y proporciona la hora al sistema operativo.
- Intervalo de sondeo especial: hace comprobaciones en el servidor NTP configurado cada 900 segundos (15 minutos).

Ruta de registro	Nombre de la clave	Datos
HKLM:\System\CurrentControlSet\services\w32time\Config	UpdateInterval	120

Ruta de registro	Nombre de la clave	Datos
HKLM:\System\CurrentControlSet\services\w32time\Parameters	NtpServer	169.254.169.123,0x9
HKLM:\System\CurrentControlSet\services\w32time\Parameters	Tipo	NTP
HKLM:\System\CurrentControlSet\services\w32time\TimeProviders\NtpClient	Habilitado	1
HKLM:\System\CurrentControlSet\services\w32time\TimeProviders\NtpClient	InputProvider	1
HKLM:\System\CurrentControlSet\services\w32time\TimeProviders\NtpClient	SpecialPollInterval	900

Conexión al punto de conexión de IPv6 del Servicio de sincronización temporal de Amazon

En esta sección se explica en qué difieren los pasos descritos en Conexión al punto de conexión de IPv4 del Servicio de sincronización temporal de Amazon si configura su instancia de modo que use el Servicio de sincronización temporal de Amazon local a través del punto de conexión IPv6. No se explica todo el proceso de configuración de Servicio de sincronización temporal de Amazon.

Solo se puede acceder al punto de conexión IPv6 en instancias integradas en el AWS Nitro System.

> **Note**
>
> No se recomienda utilizar juntas las entradas del punto de conexión IPv4 e IPv6. Los paquetes NTP de IPv4 e IPv6 provienen del mismo servidor local para su instancia. No es necesario configurar los puntos de conexión de IPv4 e IPv6 y esto no mejorará la precisión de la hora de la instancia.

Consulte las instrucciones del sistema operativo de su instancia.

Linux

En función de la distribución de Linux que utilice, cuando llegue al paso para editar el archivo chrony.conf, utilizará el punto de conexión IPv6 del Servicio de sincronización temporal de Amazon (`fd00:ec2::123`) en lugar del punto de conexión IPv4 (`169.254.169.123`):

```
server fd00:ec2::123 prefer iburst minpoll 4 maxpoll 4
```

Guarde el archivo y verifique que `chrony` esté utilizando el punto de conexión IPv6 `fd00:ec2::123` para sincronizar la hora:

```
[ec2-user ~]$ chronyc sources -v
```

Si ve el punto de conexión IPv6 `fd00:ec2::123` en la salida, la configuración está completa.

Windows

Cuando llegue al paso para cambiar el servidor NTP para que utilice el Servicio de sincronización temporal de Amazon, utilizará el punto de conexión IPv6 del Servicio de sincronización temporal de Amazon (`fd00:ec2::123`) en lugar del punto de conexión IPv4 (`169.254.169.123`):

```
w32tm /config /manualpeerlist:fd00:ec2::123 /syncfromflags:manual /update
```

Compruebe que la nueva configuración utilice el punto de conexión IPv6 `fd00:ec2::123` para sincronizar la hora:

```
w32tm /query /configuration
```

En la salida, verifique que `NtpServer` muestra el punto de conexión IPv6 `fd00:ec2::123`.

Conexión al reloj de hardware de PTP

El reloj de hardware de PTP forma parte del AWS Nitro System, por lo que se puede acceder a él directamente en las instancias de EC2 virtualizadas y bare metal admitidas sin necesidad de utilizar ningún recurso del cliente.

Los puntos de conexión NTP del reloj de hardware de PTP son los mismos que los de la conexión normal del Servicio de sincronización temporal de Amazon a través de IPv4 o IPv6. Si el software

está configurado para el punto de conexión NTP y se ejecuta en una instancia con un reloj de hardware de PTP, se conectará al reloj de hardware de PTP automáticamente a través de NTP.

Requisitos

El reloj de hardware de PTP está disponible en una instancia cuando se cumplen los siguientes requisitos:

- Compatible con las Regiones de AWS: Este de EE. UU. (Norte de Virginia) y Asia-Pacífico (Tokio)
- Familias de instancias admitidas:
  - De uso general: M7a, M7g, M7gd, M7i
  - Optimizadas para la computación: C7a, C7gd, C7i
  - Optimizadas para la memoria: R7a, R7g, R7gd, R7i
- (Solo Linux) El controlador de ENA, versión 2.10.0 o posteriores, está instalado en un sistema operativo compatible. Para obtener más información sobre los sistemas operativos compatibles, consulte los requisitos previos del controlador en GitHub.

Consulte las instrucciones del sistema operativo de su instancia.

Linux

En esta sección, se describe cómo configurar la instancia para que utilice el Servicio de sincronización temporal de Amazon local a través del reloj de hardware de PTP mediante una conexión PTP directa. Es necesario agregar una entrada de servidor para el reloj de hardware PTP al archivo de configuración `chrony`.

Si la instancia tiene un reloj de hardware de PTP y configuró la conexión NTP (al punto de conexión IPv4 o IPv6), la hora de la instancia se obtiene automáticamente del reloj de hardware de PTP. Los pasos que se indican a continuación configuran la conexión PTP directa, lo que le proporcionará una hora más precisa que la conexión NTP.

Conexión al reloj de hardware de PTP

1. Conéctese a su instancia e instale el controlador del kernel de Linux para la versión 2.10.0 o posteriores de Elastic Network Adapter (ENA). Para ver las instrucciones de instalación, consulte Linux kernel driver for Elastic Network Adapter (ENA) family en GitHub.
2. Compruebe que el dispositivo `/dev/ptp0` aparezca en su instancia.

```
[ec2-user ~]$ ls /dev/ptp0
```

El resultado esperado es el siguiente. Si `/dev/ptp0` no está en la salida, significa que el controlador de ENA no se instaló correctamente. Revise el paso 1 de este procedimiento para instalar el controlador.

```
/dev/ptp0
```

3. Edite `/etc/chrony.conf` con un editor de texto y agregue la siguiente línea en cualquier parte del archivo.

```
refclock PHC /dev/ptp0 poll 0 delay 0.000010 prefer
```

4. Reinicie chrony con el siguiente comando.

```
[ec2-user ~]$ sudo systemctl restart chronyd
```

5. Compruebe que chrony utilice el reloj de hardware de PTP para sincronizar la hora en esta instancia.

```
[ec2-user ~]$ chronyc sources
```

Resultado previsto

```
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
#* PHC0                          0   0    377    1   +2ns[ +1ns] +/-   5031ns
```

En la respuesta obtenida, * indica el origen de hora preferido. `PHC0` corresponde al reloj de hardware de PTP. Puede que tenga que esperar unos segundos después de reiniciar chrony para que aparezca el asterisco.

Windows

Las instancias de Windows solo admiten una conexión NTP al reloj de hardware de PTP local.

Los puntos de conexión NTP del reloj de hardware de PTP son los mismos que los de la conexión normal del Servicio de sincronización temporal de Amazon a través de IPv4 o IPv6. Si el software

está configurado para conectarse a un punto de conexión NTP y se ejecuta en una instancia con un reloj de hardware de PTP, se conectará al reloj de hardware de PTP a través de NTP.

Configuración de una instancia o cualquier dispositivo conectado a Internet para usar el Servicio de sincronización temporal de Amazon público

Puede configurar su instancia, o cualquier dispositivo conectado a Internet, como un ordenador local o un servidor en las instalaciones, para que utilice el Servicio de sincronización temporal de Amazon público, al que se puede acceder a través de Internet en `time.aws.com`. Puede usar el Servicio de sincronización temporal de Amazon público como una copia de seguridad para el Servicio de sincronización temporal de Amazon local y para conectar recursos ajenos a AWS al Servicio de sincronización temporal de Amazon.

> **Note**
>
> Para obtener el mejor rendimiento, le recomendamos que utilice el Servicio de sincronización temporal de Amazon local en sus instancias y que solo utilice el Servicio de sincronización temporal de Amazon público como respaldo.

Consulte las instrucciones del sistema operativo de su instancia o dispositivo.

Linux

Configuración de una instancia o dispositivo de Linux para que utilice el Servicio de sincronización temporal de Amazon público mediante chrony o ntpd

1. Edite `/etc/chrony.conf` (si usa chrony) o `/etc/ntp.conf` (si usa ntpd) con un editor de texto como se explica a continuación:

   a. Elimine o comente otras líneas que empiecen por `server` excepto las conexiones existentes al Servicio de sincronización temporal de Amazon local para evitar que su instancia o dispositivo intente mezclar servidores extendidos y no extendidos.

      > **Important**
      >
      > Si está configurando su instancia de EC2 para que se conecte al Servicio de sincronización temporal de Amazon público, no elimine la siguiente línea, que indica que su instancia se conectará al Servicio de sincronización temporal de Amazon

local. El Servicio de sincronización temporal de Amazon local es una conexión más directa y proporcionará una mayor precisión del reloj. El Servicio de sincronización temporal de Amazon público solo debe usarse como copia de seguridad.

```
server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
```

b. Agregue la siguiente línea para conectarse al Servicio de sincronización temporal de Amazon público.

```
pool time.aws.com iburst
```

2. Reinicie el daemon con uno de los siguientes comandos:

   - chrony

   ```
   sudo service chronyd force-reload
   ```

   - ntpd

   ```
   sudo service ntp reload
   ```

macOS

Configuración de una instancia o dispositivo de macOS para que utilice el Servicio de sincronización temporal de Amazon público

1. Abra Preferencias del sistema.
2. Elija Date & Time (Fecha y hora) y, a continuación, la pestaña Date & Time (Fecha y hora).
3. Para hacer cambios, elija el icono del candado e ingrese la contraseña cuando se le solicite.
4. En Set date and time automatically (Establecer fecha y hora automáticamente), ingrese **`time.aws.com`**.

Windows

Configuración de una instancia o dispositivo de Windows para que utilice el Servicio de sincronización temporal de Amazon público

1. Abra Control Panel (Panel de control).
2. Seleccione el icono de Date and Time (Fecha y hora).
3. Seleccione la pestaña Internet Time (Hora de Internet). Esta pestaña no estará disponible si su PC forma parte de un dominio. En este caso, sincronizará la hora con el controlador de dominio. Puede configurar el controlador para que utilice el Servicio de sincronización temporal de Amazon público.
4. Elija Change settings (Cambiar configuración).
5. Seleccione la casilla Synchronize with an Internet time server (Sincronizar con un servidor horario de Internet).
6. Junto a Server (Servidor), escriba **`time.aws.com`**.

Configuración de una instancia o dispositivo de Windows Server para que utilice el Servicio de sincronización temporal de Amazon público

- Siga las instrucciones de Microsoft para actualizar el registro.

Compare las marcas temporales de sus instancias Linux

Si está usando el Servicio de sincronización temporal de Amazon, puede comparar las marcas de tiempo de las instancias Linux de Amazon EC2 con ClockBound para determinar la hora real de un evento. ClockBound mide la precisión del reloj de la instancia de EC2 y le permite comprobar si una marca de tiempo determinada se encuentra en el pasado o en el futuro con respecto al reloj actual de la instancia. Esta información es valiosa para determinar el orden y la coherencia de los eventos y las transacciones en las instancias de EC2, independientemente de la ubicación geográfica de cada instancia.

ClockBound es una biblioteca y daemon de código abierto. Para obtener más información sobre ClockBound, incluidas las instrucciones de instalación, consulte ClockBound en GitHub.

ClockBound solo se admite para las instancias de Linux.

Si utiliza la conexión PTP directa al reloj del hardware de PTP, su daemon de hora, como chrony, subestimará el límite de error del reloj. Esto se debe a que un reloj de hardware de PTP no transmite la información correcta del límite de error a chrony, como lo hace NTP. Como resultado, el daemon de sincronización de relojes asume que el reloj tiene una precisión de UTC y, por lo tanto, tiene un límite de error de `0`. Para medir todo el límite de errores, Nitro System calcula el límite de error del reloj de equipo de PTP y lo pone a disposición de la instancia de EC2 a través del sistema de archivos `sysfs` del controlador de ENA. Puede leerlo directamente como un valor, en nanosegundos.

Para recuperar el enlace de error del reloj de equipo de PTP

1. Primero, obtenga la ubicación correcta del dispositivo de reloj de equipo PTP mediante uno de los siguientes comandos. La ruta del comando es diferente en función de la AMI utilizada para iniciar la instancia.

   - En Amazon Linux 2:

     ```
     cat /sys/class/net/eth0/device/uevent | grep PCI_SLOT_NAME
     ```

   - En Amazon Linux 2023:

     ```
     cat /sys/class/net/ens5/device/uevent | grep PCI_SLOT_NAME
     ```

   La salida es el nombre de la ranura PCI, que es la ubicación del dispositivo de reloj de equipo de PTP. En este ejemplo, la ubicación es `0000:00:03.0`.

   ```
   PCI_SLOT_NAME=0000:00:03.0
   ```

2. Para recuperar el enlace de error del reloj de equipo de PTP, ejecute el siguiente comando. Incluya el nombre de la ranura PCI del paso anterior.

   ```
   cat /sys/bus/pci/devices/0000:00:03.0/phc_error_bound
   ```

   El resultado es el límite de error del reloj del hardware de PTP, en nanosegundos.

Para calcular el límite de error del reloj correcto en un momento específico cuando se utiliza la conexión PTP directa al reloj del hardware de PTP, debe agregar el límite de error del reloj

desde chrony o ClockBound en el momento en que chrony sondea el reloj del hardware de PTP. Para obtener más información sobre la medición y la supervisión de la precisión del reloj, consulte Administración de la precisión del reloj de instancias de Amazon EC2 con el Servicio de sincronización temporal de Amazon y Amazon CloudWatch – Parte 1.

Cambio de la zona horaria en una instancia

Las instancias de Amazon EC2 se establecen en la zona horaria UTC (hora universal coordinada) de forma predeterminada. Puede cambiar la hora de una instancia a la zona horaria local o a otra zona horaria de la red.

Consulte las instrucciones del sistema operativo de su instancia.

Linux

> **Important**
>
> Esta información se aplica a Amazon Linux. Para obtener información acerca de otras distribuciones, consulte la documentación específica.

Para cambiar la zona horaria en una instancia de AL2023 o Amazon Linux 2

1. Vea la configuración de zona horaria actual del sistema.

```
[ec2-user ~]$ timedatectl
```

2. Enumere las zonas horarias disponibles.

```
[ec2-user ~]$ timedatectl list-timezones
```

3. Configure la zona horaria elegida.

```
[ec2-user ~]$ sudo timedatectl set-timezone America/Vancouver
```

4. (Opcional) Confirme que la zona horaria actual se ha actualizado a la nueva zona horaria al usar de nuevo el comando timedatectl.

```
[ec2-user ~]$ timedatectl
```

Para cambiar la zona horaria en una instancia de Amazon Linux

1. Identifique la zona horaria que usar en la instancia. El directorio `/usr/share/zoneinfo` contiene una jerarquía de los archivos de datos de las zonas horarias. Explore la estructura de directorios de esa ubicación para buscar un archivo para su zona horaria.

```
[ec2-user ~]$ ls /usr/share/zoneinfo
Africa      Chile    GB         Indian       Mideast   posixrules  US
America     CST6CDT  GB-Eire    Iran         MST       PRC         UTC
Antarctica  Cuba     GMT        iso3166.tab  MST7MDT   PST8PDT     WET
Arctic      EET      GMT0       Israel       Navajo    right       W-SU
...
```

   Algunas entradas de esta ubicación son directorios (como `America`) y esos directorios contienen archivos de zona horaria para ciudades específicas. Busque la ciudad (o una ciudad en la zona horaria) para usar en la instancia.

2. Actualice el archivo `/etc/sysconfig/clock` con la nueva zona horaria. En este ejemplo, utilizamos el archivo de datos de la zona horaria para Los Ángeles, `/usr/share/zoneinfo/America/Los_Angeles`.

   a. Abra el archivo `/etc/sysconfig/clock` con un editor de texto (como vim o nano). Debe utilizar sudo con el comando del editor porque `/etc/sysconfig/clock` es el propietario de `root`.

```
[ec2-user ~]$ sudo nano /etc/sysconfig/clock
```

   b. Localice la entrada `ZONE` y cámbiela por el archivo de zona horaria (omitiendo la sección `/usr/share/zoneinfo` de la ruta). Por ejemplo, para cambiar a la zona horaria de Los Ángeles, cambie la entrada `ZONE` por lo siguiente:

```
ZONE="America/Los_Angeles"
```

> **Note**
>
> No cambie la entrada `UTC=true` por otro valor. Esta entrada es para el reloj de hardware y no necesita ajustarse cuando establece una zona horaria diferente en la instancia.

c. Guarde el archivo y salga del editor de texto.

3. Cree un enlace simbólico entre `/etc/localtime` y el archivo de zona horaria de manera que la instancia lo encuentre cuando haga referencia a la información de hora local.

```
[ec2-user ~]$ sudo ln -sf /usr/share/zoneinfo/America/Los_Angeles /etc/localtime
```

4. Vuelva a arrancar el sistema para actualizar la nueva información de zona horaria en todos los servicios y aplicaciones.

```
[ec2-user ~]$ sudo reboot
```

5. (Opcional) Confirme que la zona horaria actual se ha actualizado a la nueva zona horaria mediante el comando date. La zona horaria actual aparece en la salida. En el siguiente ejemplo, la zona horaria actual es PDT, que hace referencia a la zona horaria de Los Ángeles.

```
[ec2-user ~]$ date
Sun Aug 16 05:45:16 PDT 2020
```

Windows

Cambio de la zona horaria en una instancia de Windows

1. Desde la instancia, abra una ventana del símbolo del sistema.
2. Identifique la zona horaria que usar en la instancia. Para obtener una lista de zonas horarias, utilice el siguiente comando:

```
tzutil /l
```

Este comando devuelve una lista de todas las zonas horarias disponibles, con el siguiente formato:

```
display name
time zone ID
```

3. Encuentre el ID de zona horaria que asignar a la instancia.
4. Realice la asignación a otra zona horaria con el siguiente comando:

```
tzutil /s "Pacific Standard Time"
```

La nueva zona horaria debe surtir efecto de inmediato.

> **Note**
>
> Puede asignar la zona horaria UTC mediante el siguiente comando:
>
> ```
> tzutil /s "UTC"
> ```

Prevención de que una zona horaria cambie una vez que se haya configurado para Windows Server

Cuando cambia la zona horaria en una instancia de Windows, debe asegurarse de que la zona horaria persista a través de los reinicios del sistema. En caso contrario, cuando la instancia se reinicia, se revierten los cambios y vuelve a usar la hora UTC. Puede persistir la configuración de la zona horaria si agrega una clave de registro RealTimeIsUniversal. Esta clave se establece de forma predeterminada en todas las instancias de generación actual. Para verificar si la clave de registro RealTimeIsUniversal está establecida, consulte el paso 4 en el siguiente procedimiento. Si la clave no está establecida, siga estos pasos desde el principio.

Para establecer la clave del registro RealTimeIsUniversal

1. Desde la instancia, abra una ventana del símbolo del sistema.
2. Utilice el siguiente comando para añadir la clave del registro:

   ```
   reg add "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation" /
   v RealTimeIsUniversal /d 1 /t REG_DWORD /f
   ```
3. Si está utilizando una AMI de Windows Server 2008 (no de Windows Server 2008 R2) creada antes del 22 de febrero de 2013, es recomendable que actualice a la última AMI de Windows de AWS. Si está utilizando una AMI que ejecuta Windows Server 2008 R2 (no Windows Server 2008), debe comprobar que está instalado el hotfix de Microsoft KB2922223. Si este hotfix no está instalado, recomendamos actualizar a la última AMI para Windows de AWS.
4. (Opcional) Compruebe que la instancia guardó la clave correctamente mediante el siguiente comando:

```
reg query "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control
\TimeZoneInformation" /s
```

Este comando devuelve las subclaves de la clave TimeZoneInformation del registro. Debería ver la clave RealTimeIsUniversal en la parte inferior de la lista, como se muestra a continuación:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation
    Bias                            REG_DWORD     0x1e0
    DaylightBias                    REG_DWORD     0xffffffc4
    DaylightName                    REG_SZ        @tzres.dll,-211
    DaylightStart                   REG_BINARY    00000300020002000000000000000000
    StandardBias                    REG_DWORD     0x0
    StandardName                    REG_SZ        @tzres.dll,-212
    StandardStart                   REG_BINARY    00000B0001000200000000000000000
    TimeZoneKeyName                 REG_SZ        Pacific Standard Time
    DynamicDaylightTimeDisabled     REG_DWORD     0x0
    ActiveTimeBias                  REG_DWORD     0x1a4
    RealTimeIsUniversal             REG_DWORD     0x1
```

Segundos intercalares

Los segundos intercalares, introducidos en 1972, son ajustes ocasionales de un segundo en la hora UTC para tener en cuenta las irregularidades en la rotación de la Tierra y tener en cuenta las diferencias entre la hora atómica internacional (TAI) y la hora solar (Ut1). Para administrar los segundos intercalares en beneficio de los clientes, hemos diseñado la difuminación de segundos intercalares en el Servicio de sincronización temporal de Amazon. Para obtener más información, consulte Look Before You Leap – The Coming Leap Second and AWS.

Los segundos intercalares están desapareciendo y apoyamos plenamente la decisión tomada en la 27.ª conferencia general sobre ponderaciones y medidas para abandonar los segundos intercalares a más tardar en 2035.

Para respaldar esta transición, seguimos pensando en la difuminación temporal durante un evento de segundo intercalar al acceder al Servicio de sincronización temporal de Amazon a través de la conexión NTP local o de nuestros grupos NTP públicos (`time.aws.com`). Sin embargo, el reloj de hardware de PTP no ofrece una opción de tiempo extendido. En caso de un segundo intercalar, el reloj de hardware de PTP agregará el segundo intercalar siguiendo los estándares de UTC. Los orígenes de tiempo con difuminación temporal y segundos intercalares son iguales en la mayoría

de los casos. Sin embargo, debido a que difieren durante un evento de segundo intercalar, no recomendamos utilizar orígenes de tiempo difuminados y no difuminados en la configuración de su cliente de tiempo durante un evento de segundo intercalar.

Recursos relacionados

- AWS Blog de computación: Ya era hora: relojes con una precisión de microsegundos en las instancias de Amazon EC2
- (Linux) https://chrony-project.org/
- (Windows) How the Windows Time Service Works (Microsoft)
- (Windows) W32tm (Microsoft)
- (Windows) How the Windows Time service treats a leap second (Microsoft)
- (Windows) The story around Leap Seconds and Windows: It's likely not Y2K (Microsoft)

Control de los estados del procesador de la instancia de Amazon EC2 Linux

Los estados C controlan los niveles de suspensión en los que puede entrar el núcleo cuando está inactivo. Los estados C se enumeran comenzando por C0 (el estado menos profundo, cuando el núcleo está totalmente activo y ejecutando instrucciones) y hasta C6 (el estado de inactividad más profundo en el que el núcleo está desactivado).

Los estados P controlan el rendimiento deseado (en frecuencia de CPU) desde un núcleo. Los estados P se enumeran comenzando por P0 (el ajuste de rendimiento más alto con el que el núcleo puede utilizar la tecnología Intel Turbo Boost Technology para aumentar la frecuencia si es posible) y van de P1 (el estado P que solicita la frecuencia básica máxima) hasta P15 (la frecuencia más baja posible).

Estados C y estados P

Los siguientes tipos de instancias ofrecen la capacidad de que un sistema operativo controle los estados C y P del procesador:

- De uso general: `m4.10xlarge` | `m4.16xlarge` | `m5.metal` | `m5d.metal` | `m5n.metal` | `m5zn.metal` | `m6i.metal` | `m6id.metal` | `m7a.metal-48xl` | `m7i.metal-24xl` | `m7i.metal-48xl`

- Optimizadas para computación: c4.8xlarge | c5.metal | c5an.metal | c5adn.metal | c5n.metal | c6i.metal | c6id.metal | c7a.metal-48xl | c7i.metal-24xl | c7i.metal-48xl
- Optimizadas para memoria: r4.8xlarge | r4.16xlarge | r5.metal | r5b.metal | r5d.metal | r6i.metal | r7a.metal-48xl | r7i.metal-24xl | r7i.metal-48xl | r7iz.metal-16xl | r7iz.metal-32xl | u-6tb1.metal | u-9tb1.metal | u-12tb1.metal | u-18tb1.metal | u-24tb1.metal | x1.16xlarge | x1.32xlarge | x1e.8xlarge | x1e.16xlarge | x1e.32xlarge | z1d.metal
- Optimizadas para almacenamiento: d2.8xlarge | d3.metal | d3en.metal | i3.8xlarge | i3.16xlarge | i3.metal | i3en.metal | h1.8xlarge | h1.16xlarge
- Computación acelerada: f1.16xlarge | g3.16xlarge | g4dn.metal | p2.16xlarge | p3.16xlarge

Solo en estados C

Los siguientes tipos de instancias ofrecen la capacidad de que un sistema operativo controle los estados C del procesador:

- De uso general: m5.12xlarge | m5.24xlarge | m5d.12xlarge | m5d.24xlarge | m5n.12xlarge | m5n.24xlarge | m5dn.12xlarge | m5dn.24xlarge | m6a.24xlarge | m6a.48xlarge | m6ad.metal | m6i.16xlarge | m6i.32xlarge | m7a.medium | m7a.large | m7a.xlarge | m7a.2xlarge | m7a.4xlarge | m7a.8xlarge | m7a.12xlarge | m7a.16xlarge | m7a.24xlarge | m7a.32xlarge | m7a.48xlarge | m7i.large | m7i.xlarge | m7i.2xlarge | m7i.4xlarge | m7i.8xlarge | m7i.12xlarge | m7i.16xlarge | m7i.24xlarge | m7i.48xlarge
- Optimizadas para computación: c5.9xlarge | c5.12xlarge | c5.18xlarge | c5.24xlarge | c5a.24xlarge | c5ad.24xlarge | c5d.9xlarge | c5d.12xlarge | c5d.18xlarge | c5d.24xlarge | c5n.9xlarge | c5n.18xlarge | c6a.24xlarge | c6a.32xlarge | c6a.48xlarge | c6i.16xlarge | c6i.32xlarge | c7a.medium | c7a.large | c7a.xlarge | c7a.2xlarge | c7a.4xlarge | c7a.8xlarge | c7a.12xlarge | c7a.16xlarge | c7a.24xlarge | c7a.32xlarge | c7a.48xlarge | c7i.large | c7i.xlarge | c7i.2xlarge | c7i.4xlarge | c7i.8xlarge | c7i.12xlarge | c7i.16xlarge | c7i.24xlarge | c7i.48xlarge
- Optimizadas para memoria: r5.12xlarge | r5.24xlarge | r5d.12xlarge | r5d.24xlarge | r5n.12xlarge | r5n.24xlarge | r5dn.12xlarge | r5dn.24xlarge |r6a.24xlarge | r6a.48xlarge | r6i.16xlarge | r6i.32xlarge | r6id.32xlarge | r6in.32xlarge |

`r7a.medium` | `r7a.large` | `r7a.xlarge` | `r7a.2xlarge` | `r7a.4xlarge` | `r7a.8xlarge` | `r7a.12xlarge` | `r7a.16xlarge` | `r7a.24xlarge` | `r7a.32xlarge` | `r7a.48xlarge` | `r7i.large` | `r7i.xlarge` | `r7i.2xlarge` | `r7i.4xlarge` | `r7i.8xlarge` | `r7i.12xlarge` | `r7i.16xlarge` | `r7i.24xlarge` | `r7i.48xlarge` | `r7iz.large` | `r7iz.xlarge` | `r7iz.2xlarge` | `r7iz.4xlarge` | `r7iz.8xlarge` | `r7iz.12xlarge` | `r7iz.16xlarge` | `r7iz.32xlarge` | `u-6tb1.56xlarge` | `u-6tb1.112xlarge` | `u-9tb1.112xlarge` | `u-12tb1.112xlarge` | `u-18tb1.112xlarge` | `u-24tb1.112xlarge` | `u7i-12tb.224xlarge` | `u7in-16tb.224xlarge` | `u7in-24tb.224xlarge` | `u7in-32tb.224xlarge` | `z1d.6xlarge` | `z1d.12xlarge`

- Optimizado para almacenamiento: `d3en.12xlarge` | `dl1.24xlarge` | `i3en.12xlarge` | `i3en.24xlarge` | `i4i.metal` | `r5b.12xlarge` | `r5b.24xlarge` | `i4i.16xlarge`
- Computación acelerada: `dl1.24xlarge` | `g5.24xlarge` | `g5.48xlarge` | `g6.24xlarge` | `g6.48xlarge` | `inf1.24xlarge` | `p3dn.24xlarge` | `p4d.24xlarge` | `p4de.24xlarge` | `vt1.24xlarge`

Los procesadores AWS Graviton tienen modos de ahorro de energía integrados y funcionan a una frecuencia fija. Por lo tanto, no proporcionan la capacidad del sistema operativo para controlar los estados C y P.

Es posible que desee cambiar los ajustes del estado C o P para aumentar la uniformidad del rendimiento del procesador, reducir la latencia o ajustar la instancia para una carga de trabajo concreta. Los ajustes de estado C y P predeterminados ofrecen un rendimiento máximo, que es óptimo para la mayoría de cargas de trabajo. Sin embargo, si la aplicación puede beneficiarse de una latencia reducida a costa de frecuencias superiores de núcleo doble o único, o de un rendimiento uniforme a frecuencias más bajas en lugar de frecuencias por ráfagas Turbo Boost, plantéese experimentar con los ajustes de estado C o P disponibles para estas instancias.

Para acceder a información sobre las distintas configuraciones del procesador y aprender a supervisar los efectos de la configuración para Amazon Linux, consulte Processor state control for Amazon EC2 Amazon Linux instance en la Guía del usuario de Amazon Linux 2. Estos procedimientos se han escrito para Amazon Linux y se aplican a él; sin embargo, también pueden funcionar para otras distribuciones de Linux con un kernel de Linux 3.9 o posterior. Para obtener más información acerca de otras distribuciones de Linux y el control de estados del procesador, consulte la documentación específica de su sistema.

Optimización de las opciones de CPU

Muchas de las instancias Amazon EC2 admiten el multiproceso simultáneo, lo que permite la ejecución simultánea de varios subprocesos en un único núcleo de CPU. Cada subproceso está representado como una CPU virtual (vCPU) en la instancia. Una instancia tiene un número predeterminado de núcleos de CPU, que varía en función del tipo de instancia. Por ejemplo, el tipo de instancia `m5.xlarge` tiene dos núcleos de CPU y dos subprocesos por núcleo de forma predeterminada, es decir,— cuatro CPU virtuales en total.

> **Note**
>
> Cada vCPU es un subproceso de un núcleo de CPU, excepto para las instancias T2, las instancias M7a, las instancias de Apple Silicon Mac y las plataformas ARM de 64 bits, como las instancias con procesadores de AWS Graviton.

En la mayoría de los casos, habrá un tipo de instancia Amazon EC2 con la combinación de memoria y número de vCPU adecuada para sus cargas de trabajo. Sin embargo, puede especificar las siguientes opciones de CPU para optimizar la instancia en función de cargas de trabajo o necesidades empresariales específicas:

- Número de núcleos de CPU: puede personalizar el número de núcleos de CPU de la instancia. Esto le ofrecerá la posibilidad de optimizar los costos de licencias de software con una instancia que dispone de la cantidad suficiente de memoria RAM para cargas de trabajo con uso intensivo de memoria pero menos núcleos de CPU.
- Subprocesos por núcleo: puede deshabilitar el multiproceso especificando un único subproceso por núcleo de CPU. Esto podría utilizarlo en determinadas cargas de trabajo, como las cargas de trabajo de informática de alto rendimiento (HPC).

Puede especificar estas opciones de CPU durante la inicialización de la instancia. No se aplican cargos adicionales o reducidos al especificar opciones de CPU. Se aplican los mismos cargos que en el caso de las instancias que se inician con opciones de CPU predeterminadas.

Contenido

- Visualizar las opciones de CPU de una instancia

Reglas para especificar opciones de CPU

Tenga en cuenta las siguientes reglas al especificar las opciones de CPU para la instancia:

- No puede especificar las opciones de CPU para las instancias bare metal.
- Las opciones de CPU solo se pueden especificar durante la inicialización de la instancia y no se podrán modificar posteriormente.
- Al iniciar una instancia, es necesario especificar el número de núcleos de CPU y subprocesos por núcleo en la solicitud. Para obtener ejemplos de solicitudes, consulte Especificar opciones de CPU para una instancia.
- La cantidad de CPU virtuales de la instancia es el número de núcleos de CPU multiplicado por el número de subprocesos por núcleo. Para especificar un número personalizado de vCPU, es necesario especificar un número válido de núcleos de CPU y subprocesos para el tipo de instancia. No puede superar el número predeterminado de vCPU de la instancia. Para obtener más información, consulte Núcleos de CPU y subprocesos por núcleo de CPU por tipo de instancia.
- Para deshabilitar el multiproceso, especifique un subproceso por núcleo.
- Si cambia el tipo de instancia de una instancia existente, las opciones de CPU se reemplazan automáticamente por las opciones de CPU predeterminadas del nuevo tipo de instancia.
- Las opciones de CPU especificadas se conservarán al detener, iniciar o reiniciar una instancia.

Núcleos de CPU y subprocesos por núcleo de CPU por tipo de instancia

Las tablas siguientes muestran los tipos de instancia que admiten la especificación de opciones de CPU.

Contenido

instancias de uso general

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
m2.xlarge	2	2	1	1, 2	1
m2.2xlarge	4	4	1	1, 2, 3, 4	1
m2.4xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m3.large	2	1	2	1	1, 2
m3.xlarge	4	2	2	1, 2	1, 2
m3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m4.large	2.	1	2	1	1, 2
m4.xlarge	4	2	2	1, 2	1, 2
m4.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m4.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m4.10xlarge	40	20	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20	1, 2
m4.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22,	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
				24, 26, 28, 30, 32	
m5.large	2.	1	2	1	1, 2
m5.xlarge	4	2	2	2	1, 2
m5.2xlarge	8	4	2	2, 4	1, 2
m5.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m5.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m5.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
m5a.large	2.	1	2	1	1, 2
m5a.xlarge	4	2	2	2	1, 2
m5a.2xlarge	8	4	2	2, 4	1, 2
m5a.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
m5a.12xlarge	48	24	2	6, 12, 18, 24	1, 2
m5a.16xlarge	64	32	2	8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5a.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
m5ad.large	2.	1	2	1	1, 2
m5ad.xlarge	4	2	2	2	1, 2
m5ad.2xlarge	8	4	2	2, 4	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
m5ad.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5ad.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
m5ad.12xlarge	48	24	2	6, 12, 18, 24	1, 2
m5ad.16xlarge	64	32	2	8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5ad.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
m5d.large	2.	1	2	1	1, 2
m5d.xlarge	4	2	2	2	1, 2
m5d.2xlarge	8	4	2	2, 4	1, 2
m5d.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5d.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m5d.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
m5d.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5d.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5dn.large	2.	1	2	1	1, 2
m5dn.xlarge	4	2	2	1, 2	1, 2
m5dn.2xlarge	8	4	2	2, 4	1, 2
m5dn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5dn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m5dn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
m5dn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5dn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5n.large	2.	1	2	1	1, 2
m5n.xlarge	4	2	2	1, 2	1, 2
m5n.2xlarge	8	4	2	2, 4	1, 2
m5n.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5n.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m5n.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
m5n.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5n.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5zn.large	2.	1	2	1	1, 2
m5zn.xlarge	4	2	2	1, 2	1, 2
m5zn.2xlarge	8	4	2	2, 4	1, 2
m5zn.3xlarge	12	6	2	2, 4, 6	1, 2
m5zn.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
m5zn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
m6a.large	2.	1	2	1	1, 2
m6a.xlarge	4	2	2	1, 2	1, 2
m6a.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m6a.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m6a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
m6a.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 16, 24	1, 2
m6a.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 32	1, 2
m6a.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 32, 48	1, 2
m6a.32xlarge	128	64	2	8, 12, 16, 20, 24, 28, 32, 64	1, 2
m6a.48xlarge	192	96	2	8, 12, 16, 20, 24, 28, 32, 64, 96	1, 2
m6g.large	2	2	1	1, 2	1

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
m6g.xlarge	4	4	1	1, 2, 3, 4	1
m6g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m6g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m6g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
m6g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
m6g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
m6gd.large	2	2	1	1, 2	1
m6gd.xlarge	4	4	1	1, 2, 3, 4	1
m6gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
m6gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m6gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
m6gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
m6gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
m6i.large	2	1	2	1	1, 2
m6i.xlarge	4	2	2	1, 2	1, 2
m6i.2xlarge	8	4	2	2, 4	1, 2
m6i.4xlarge	16	8	2	2, 4, 6, 8	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
m6i.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m6i.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m6i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m6i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m6i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
m6id.large	2.	1	2	1	1, 2
m6id.xlarge	4	2	2	1, 2	1, 2
m6id.2xlarge	8	4	2	2, 4	1, 2
m6id.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m6id.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m6id.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m6id.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m6id.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
m6id.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m6idn.large	2.	1	2	1	1, 2
m6idn.xlarge	4	2	2	1, 2	1, 2
m6idn.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m6idn.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m6idn.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
m6idn.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m6idn.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
m6idn.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
m6idn.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m6in.large	2.	1	2	1	1, 2
m6in.xlarge	4	2	2	1, 2	1, 2
m6in.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m6in.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m6in.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
m6in.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m6in.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
m6in.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
m6in.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m7a.large	2	2	1	1, 2	1
m7a.xlarge	4	4	1	1, 2, 3, 4	1
m7a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m7a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
m7a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
m7a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
m7a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1
m7a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1
m7a.32xlarge	128	128	1	4, 6, 8, 10, 12, 14, 16, 32, 48, 64, 80, 96, 112, 128	1
m7a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1
m7g.large	2	2	1	1, 2	1
m7g.xlarge	4	4	1	1, 2, 3, 4	1
m7g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
m7g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m7g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
m7g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
m7g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
m7gd.large	2	2	1	1, 2	1
m7gd.xlarge	4	4	1	1, 2, 3, 4	1
m7gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
m7gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m7gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
m7gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
m7gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
m7i.large	2	1	2	1	1, 2
m7i.xlarge	4	2	2	1, 2	1, 2
m7i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m7i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
m7i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
m7i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m7i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
m7i.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2
m7i.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
m7i-flex.large	2.	1	2	1	1, 2
m7i-flex.xlarge	4	2	2	1, 2	1, 2
m7i-flex.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m7i-flex.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m7i-flex.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
t3.nano	2.	1	2	1	1, 2
t3.micro	2.	1	2	1	1, 2
t3.small	2.	1	2	1	1, 2
t3.medium	2.	1	2	1	1, 2
t3.large	2.	1	2	1	1, 2
t3.xlarge	4	2	2	2	1, 2
t3.2xlarge	8	4	2	2, 4	1, 2
t3a.nano	2.	1	2	1	1, 2
t3a.micro	2.	1	2	1	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
t3a.small	2.	1	2	1	1, 2
t3a.medium	2.	1	2	1	1, 2
t3a.large	2.	1	2	1	1, 2
t3a.xlarge	4	2	2	2	1, 2
t3a.2xlarge	8	4	2	2, 4	1, 2
t4g.nano	2	2	1	1, 2	1
t4g.micro	2	2	1	1, 2	1
t4g.small	2	2	1	1, 2	1
t4g.medium	2	2	1	1, 2	1
t4g.large	2	2	1	1, 2	1
t4g.xlarge	4	4	1	1, 2, 3, 4	1
t4g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

instancias optimizadas para computación

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
c3.large	2.	1	2	1	1, 2
c3.xlarge	4	2	2	1, 2	1, 2
c3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c3.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
c4.large	2.	1	2	1	1, 2
c4.xlarge	4	2	2	1, 2	1, 2
c4.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c4.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c4.8xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5.large	2.	1	2	1	1, 2
c5.xlarge	4	2	2	2	1, 2
c5.2xlarge	8	4	2	2, 4	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
c5.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c5.9xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
c5.18xlarge	72	36	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36	1, 2
c5.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
c5a.large	2.	1	2	1	1, 2
c5a.xlarge	4	2	2	1, 2	1, 2
c5a.2xlarge	8	4	2	1, 2, 3, 4	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
c5a.4xlarge	16	8	2	1, 2, 3, 4, 8	1, 2
c5a.8xlarge	32	16	2	1, 2, 3, 4, 8, 12, 16	1, 2
c5a.12xlarge	48	24	2	1, 2, 3, 4, 8, 12, 16, 20, 24	1, 2
c5a.16xlarge	64	32	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1, 2
c5a.24xlarge	96	48	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48	1, 2
c5ad.large	2.	1	2	1	1, 2
c5ad.xlarge	4	2	2	1, 2	1, 2
c5ad.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c5ad.4xlarge	16	8	2	1, 2, 3, 4, 8	1, 2
c5ad.8xlarge	32	16	2	1, 2, 3, 4, 8, 12, 16	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
c5ad.12xlarge	48	24	2	1, 2, 3, 4, 8, 12, 16, 20, 24	1, 2
c5ad.16xlarge	64	32	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1, 2
c5ad.24xlarge	96	48	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48	1, 2
c5d.large	2.	1	2	1	1, 2
c5d.xlarge	4	2	2	2	1, 2
c5d.2xlarge	8	4	2	2, 4	1, 2
c5d.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c5d.9xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5d.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
c5d.18xlarge	72	36	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36	1, 2
c5d.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
c5n.large	2.	1	2	1	1, 2
c5n.xlarge	4	2	2	2	1, 2
c5n.2xlarge	8	4	2	2, 4	1, 2
c5n.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c5n.9xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5n.18xlarge	72	36	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
c6a.large	2.	1	2	1	1, 2
c6a.xlarge	4	2	2	1, 2	1, 2
c6a.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c6a.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c6a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
c6a.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 16, 24	1, 2
c6a.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 32	1, 2
c6a.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 32, 48	1, 2
c6a.32xlarge	128	64	2	8, 12, 16, 20, 24, 28, 32, 64	1, 2
c6a.48xlarge	192	96	2	8, 12, 16, 20, 24, 28, 32, 64, 96	1, 2
c6g.large	2	2	1	1, 2	1

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
c6g.xlarge	4	4	1	1, 2, 3, 4	1
c6g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c6g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c6g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
c6g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
c6g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c6gd.large	2	2	1	1, 2	1
c6gd.xlarge	4	4	1	1, 2, 3, 4	1
c6gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
c6gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c6gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c6gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
c6gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c6gn.medium	1	1	1	1	1
c6gn.large	2	2	1	1, 2	1
c6gn.xlarge	4	4	1	1, 2, 3, 4	1
c6gn.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
c6gn.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c6gn.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c6gn.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
c6gn.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c6i.large	2	1	2	1	1, 2
c6i.xlarge	4	2	2	1, 2	1, 2
c6i.2xlarge	8	4	2	2, 4	1, 2
c6i.4xlarge	16	8	2	2, 4, 6, 8	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
c6i.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
c6i.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
c6i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
c6i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
c6i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
c6id.large	2.	1	2	1	1, 2
c6id.xlarge	4	2	2	1, 2	1, 2
c6id.2xlarge	8	4	2	2, 4	1, 2
c6id.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c6id.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
c6id.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
c6id.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
c6id.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
c6id.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
c6in.large	2.	1	2	1	1, 2
c6in.xlarge	4	2	2	1, 2	1, 2
c6in.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c6in.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c6in.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
c6in.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
c6in.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
c6in.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
c6in.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
c7a.large	2	2	1	1, 2	1
c7a.xlarge	4	4	1	1, 2, 3, 4	1
c7a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c7a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
c7a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
c7a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
c7a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1
c7a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1
c7a.32xlarge	128	128	1	4, 6, 8, 10, 12, 14, 16, 32, 48, 64, 80, 96, 112, 128	1
c7a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1
c7g.large	2	2	1	1, 2	1
c7g.xlarge	4	4	1	1, 2, 3, 4	1
c7g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
c7g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c7g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c7g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
c7g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c7gd.large	2	2	1	1, 2	1
c7gd.xlarge	4	4	1	1, 2, 3, 4	1
c7gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
c7gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c7gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c7gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
c7gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c7gn.large	2	2	1	1, 2	1
c7gn.xlarge	4	4	1	1, 2, 3, 4	1
c7gn.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
c7gn.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c7gn.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c7gn.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
c7gn.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c7i.large	2	1	2	1	1, 2
c7i.xlarge	4	2	2	1, 2	1, 2
c7i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c7i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
c7i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
c7i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
c7i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
c7i.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2
c7i.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
c7i-flex.large	2.	1	2	1	1, 2
c7i-flex.xlarge	4	2	2	1, 2	1, 2
c7i-flex.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c7i-flex.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c7i-flex.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

instancias optimizadas para memoria

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
r3.large	2.	1	2	1	1, 2
r3.xlarge	4	2	2	1, 2	1, 2
r3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
r3.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r4.large	2.	1	2	1	1, 2
r4.xlarge	4	2	2	1, 2	1, 2
r4.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r4.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r4.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r4.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5.large	2.	1	2	1	1, 2
r5.xlarge	4	2	2	2	1, 2
r5.2xlarge	8	4	2	2, 4	1, 2
r5.4xlarge	16	8	2	2, 4, 6, 8	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
r5.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r5a.large	2.	1	2	1	1, 2
r5a.xlarge	4	2	2	2	1, 2
r5a.2xlarge	8	4	2	2, 4	1, 2
r5a.4xlarge	16	8	2	2, 4, 6, 8	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
r5a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
r5a.12xlarge	48	24	2	6, 12, 18, 24	1, 2
r5a.16xlarge	64	32	2	8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5a.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
r5ad.large	2.	1	2	1	1, 2
r5ad.xlarge	4	2	2	2	1, 2
r5ad.2xlarge	8	4	2	2, 4	1, 2
r5ad.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5ad.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
r5ad.12xlarge	48	24	2	6, 12, 18, 24	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
r5ad.16xlarge	64	32	2	8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5ad.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
r5b.large	2.	1	2	1	1, 2
r5b.xlarge	4	2	2	1, 2	1, 2
r5b.2xlarge	8	4	2	2, 4	1, 2
r5b.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5b.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5b.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5b.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
r5b.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r5d.large	2.	1	2	1	1, 2
r5d.xlarge	4	2	2	2	1, 2
r5d.2xlarge	8	4	2	2, 4	1, 2
r5d.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5d.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5d.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5d.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
r5d.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r5dn.large	2.	1	2	1	1, 2
r5dn.xlarge	4	2	2	1, 2	1, 2
r5dn.2xlarge	8	4	2	2, 4	1, 2
r5dn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5dn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5dn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5dn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
r5dn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r5n.large	2.	1	2	1	1, 2
r5n.xlarge	4	2	2	1, 2	1, 2
r5n.2xlarge	8	4	2	2, 4	1, 2
r5n.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5n.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5n.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5n.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
r5n.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r6a.large	2.	1	2	1	1, 2
r6a.xlarge	4	2	2	1, 2	1, 2
r6a.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r6a.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r6a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
r6a.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 16, 24	1, 2
r6a.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 32	1, 2
r6a.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 32, 48	1, 2
r6a.32xlarge	128	64	2	8, 12, 16, 20, 24, 28, 32, 64	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
r6a.48xlarge	192	96	2	8, 12, 16, 20, 24, 28, 32, 64, 96	1, 2
r6g.large	2	2	1	1, 2	1
r6g.xlarge	4	4	1	1, 2, 3, 4	1
r6g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r6g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r6g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
r6g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
r6g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
r6gd.large	2	2	1	1, 2	1
r6gd.xlarge	4	4	1	1, 2, 3, 4	1
r6gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
r6gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r6gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
r6gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
r6gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
r6i.large	2	1	2	1	1, 2
r6i.xlarge	4	2	2	1, 2	1, 2
r6i.2xlarge	8	4	2	2, 4	1, 2
r6i.4xlarge	16	8	2	2, 4, 6, 8	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
r6i.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r6i.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r6i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r6i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r6i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
r6idn.large	2.	1	2	1	1, 2
r6idn.xlarge	4	2	2	1, 2	1, 2
r6idn.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r6idn.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r6idn.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r6idn.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
r6idn.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
r6idn.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r6idn.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r6in.large	2.	1	2	1	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
r6in.xlarge	4	2	2	1, 2	1, 2
r6in.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r6in.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r6in.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r6in.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r6in.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
r6in.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r6in.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r6id.large	2.	1	2	1	1, 2
r6id.xlarge	4	2	2	1, 2	1, 2
r6id.2xlarge	8	4	2	2, 4	1, 2
r6id.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r6id.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
r6id.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r6id.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r6id.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r6id.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r7a.large	2	2	1	1, 2	1
r7a.xlarge	4	4	1	1, 2, 3, 4	1

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
r7a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r7a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
r7a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
r7a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1
r7a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1
r7a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1
r7a.32xlarge	128	128	1	4, 6, 8, 10, 12, 14, 16, 32, 48, 64, 80, 96, 112, 128	1

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
r7a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1
r7g.large	2	2	1	1, 2	1
r7g.xlarge	4	4	1	1, 2, 3, 4	1
r7g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r7g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r7g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
r7g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
r7g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
r7gd.large	2	2	1	1, 2	1
r7gd.xlarge	4	4	1	1, 2, 3, 4	1
r7gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
r7gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r7gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
r7gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
r7gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
r7i.large	2	1	2	1	1, 2
r7i.xlarge	4	2	2	1, 2	1, 2
r7i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r7i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
r7i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r7i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r7i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
r7i.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2
r7i.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
r7iz.large	2.	1	2	1	1, 2
r7iz.xlarge	4	2	2	1, 2	1, 2
r7iz.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r7iz.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r7iz.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r7iz.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
r7iz.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
r7iz.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
u-3tb1.56xlarge	224	112	2	4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64, 68, 72, 76, 80, 84, 88, 92, 96, 100, 104, 108, 112	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
u-6tb1.56xlarge	224	224	1	8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1
u-6tb1.112xlarge	448	224	2	8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
u-9tb1.112xlarge	448	224	2	8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2
u-12tb1.112xlarge	448	224	2	8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
u-18tb1.112xlarge	448	224	2	8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2
u-24tb1.112xlarge	448	224	2	8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
u7i-12tb.224xlarge	896	448	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 240, 248, 256, 264, 272, 280, 288, 296, 304, 312, 320, 328, 336, 344, 352, 360, 368, 376, 384, 392, 400, 408, 416, 424, 432, 440, 448	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
u7in-16tb.224xlarge	896	448	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 240, 248, 256, 264, 272, 280, 288, 296, 304, 312, 320, 328, 336, 344, 352, 360, 368, 376, 384, 392, 400, 408, 416, 424, 432, 440, 448	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
u7in-24tb.224xlarge	896	448	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 240, 248, 256, 264, 272, 280, 288, 296, 304, 312, 320, 328, 336, 344, 352, 360, 368, 376, 384, 392, 400, 408, 416, 424, 432, 440, 448	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
u7in-32tb.224xlarge	896	448	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 240, 248, 256, 264, 272, 280, 288, 296, 304, 312, 320, 328, 336, 344, 352, 360, 368, 376, 384, 392, 400, 408, 416, 424, 432, 440, 448	1, 2
x1.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
x1.32xlarge	128	64	2	4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64	1, 2
x2gd.large	2	2	1	1, 2	1
x2gd.xlarge	4	4	1	1, 2, 3, 4	1
x2gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
x2gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
x2gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
x2gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
x2gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
x2idn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
x2idn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
x2idn.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
x2iedn.xlarge	4	2	2	1, 2	1, 2
x2iedn.2xlarge	8	4	2	2, 4	1, 2
x2iedn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
x2iedn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
x2iedn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
x2iedn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
x2iedn.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
x2iezn.2xlarge	8	4	2	2, 4	1, 2
x2iezn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
x2iezn.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
x2iezn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
x2iezn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
x1e.xlarge	4	2	2	1, 2	1, 2
x1e.2xlarge	8	4	2	1, 2, 3, 4	1, 2
x1e.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
x1e.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
x1e.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
x1e.32xlarge	128	64	2	4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
z1d.large	2.	1	2	1	1, 2
z1d.xlarge	4	2	2	1, 2	1, 2
z1d.2xlarge	8	4	2	2, 4	1, 2
z1d.3xlarge	12	6	2	2, 4, 6	1, 2
z1d.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
z1d.12xlarge	48	24	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2

instancias optimizadas para almacenamiento

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
d2.xlarge	4	2	2	1, 2	1, 2
d2.2xlarge	8	4	2	1, 2, 3, 4	1, 2
d2.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
d2.8xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
d3.xlarge	4	2	2	1, 2	1, 2
d3.2xlarge	8	4	2	2, 4	1, 2
d3.4xlarge	16	8	2	2, 4, 6, 8	1, 2
d3.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
d3en.xlarge	4	2	2	1, 2	1, 2
d3en.2xlarge	8	4	2	2, 4	1, 2
d3en.4xlarge	16	8	2	2, 4, 6, 8	1, 2
d3en.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
d3en.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
d3en.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
h1.2xlarge	8	4	2	1, 2, 3, 4	1, 2
h1.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
h1.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
h1.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
i2.xlarge	4	2	2	1, 2	1, 2
i2.2xlarge	8	4	2	1, 2, 3, 4	1, 2
i2.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
i2.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
i3.large	2.	1	2	1	1, 2
i3.xlarge	4	2	2	1, 2	1, 2
i3.2xlarge	8	4	2	1, 2, 3, 4	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
i3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
i3.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
i3.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
i3en.large	2.	1	2	1	1, 2
i3en.xlarge	4	2	2	1, 2	1, 2
i3en.2xlarge	8	4	2	2, 4	1, 2
i3en.3xlarge	12	6	2	2, 4, 6	1, 2
i3en.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
i3en.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
i3en.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
i4g.large	2	2	1	1, 2	1
i4g.xlarge	4	4	1	1, 2, 3, 4	1
i4g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
i4g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
i4g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
i4g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
i4i.large	2	1	2	1	1, 2
i4i.xlarge	4	2	2	1, 2	1, 2
i4i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
i4i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
i4i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
i4i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
i4i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
i4i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
i4i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
im4gn.large	2	2	1	1, 2	1
im4gn.xlarge	4	4	1	1, 2, 3, 4	1
im4gn.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
im4gn.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
im4gn.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
im4gn.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
is4gen.medium	1	1	1	1	1
is4gen.large	2	2	1	1, 2	1
is4gen.xlarge	4	4	1	1, 2, 3, 4	1
is4gen.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
is4gen.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
is4gen.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

instancias de computación acelerada

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
dl1.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
dl2q.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
f1.2xlarge	8	4	2	1, 2, 3, 4	1, 2
f1.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
f1.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
g3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
g3.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
g3.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
g4ad.xlarge	4	2	2	2	1, 2
g4ad.2xlarge	8	4	2	2, 4	1, 2
g4ad.4xlarge	16	8	2	2, 4, 8	1, 2
g4ad.8xlarge	32	16	2	2, 4, 8, 16	1, 2
g4ad.16xlarge	64	32	2	2, 4, 8, 16, 32	1, 2
g4dn.xlarge	4	2	2	2	1, 2
g4dn.2xlarge	8	4	2	2, 4	1, 2
g4dn.4xlarge	16	8	2	2, 4, 6, 8	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
g4dn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
g4dn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
g4dn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
g5g.xlarge	4	4	1	1, 2, 3, 4	1
g5g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
g5g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
g5g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
g5g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
g6.xlarge	4	2	2	1, 2	1, 2
g6.2xlarge	8	4	2	1, 2, 3, 4	1, 2
g6.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
g6.8xlarge	32	16	2	1, 2, 4, 6, 8, 10, 12, 14, 16	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
g6.12xlarge	48	24	2	1, 2, 3, 6, 9, 12, 15, 18, 21, 24	1, 2
g6.16xlarge	64	32	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1, 2
g6.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1, 2
g6.48xlarge	192	96	2	4, 6, 8, 10, 12, 24, 36, 48, 60, 72, 84, 96	1, 2
gr6.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
gr6.8xlarge	32	16	2	1, 2, 4, 6, 8, 10, 12, 14, 16	1, 2
inf1.xlarge	4	2	2	2	1, 2
inf1.2xlarge	8	4	2	2, 4	1, 2
inf1.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
inf1.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
inf2.xlarge	4	2	2	1, 2	1, 2
inf2.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
inf2.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 32, 48	1, 2
inf2.48xlarge	192	96	2	4, 8, 12, 16, 20, 24, 28, 32, 64, 96	1, 2
p2.xlarge	4	2	2	1, 2	1, 2
p2.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
p2.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
p3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
p3.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
p3.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
p3dn.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
p4d.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
p4de.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
p5.48xlarge	192	96	2	12, 24, 36, 48, 60, 72, 84, 96	1, 2
trn1.2xlarge	8	4	2	2, 4	1, 2

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
trn1.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
trn1n.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
vt1.3xlarge	12	6	2	6	1, 2
vt1.6xlarge	24	12	2	6, 12	1, 2
vt1.24xlarge	96	48	2	6, 12, 48	1, 2

instancias de computación de alto rendimiento

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Núcleos de CPU válidos	Subprocesos válidos por núcleo
`hpc6id.32xlarge`	64	64	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1

Especificar opciones de CPU para una instancia

Puede especificar opciones de CPU durante la inicialización de la instancia.

Los siguientes ejemplos describen cómo especificar las opciones de CPU al utilizar el asistente de inicialización de instancias de la consola de EC2 y el comando run-instances de la AWS CLI, además de la página de creación de plantillas de inicialización en la consola de EC2 y el comando create-launch-template. de la AWS CLI. Para la flota de EC2 o la flota de spot, debe especificar las opciones de CPU en una plantilla de inicialización.

Los ejemplos mostrados a continuación corresponden a un tipo de instancia `r5.4xlarge`, que tiene los siguientes valores predeterminados:

- Núcleos de CPU predeterminados: 8
- Subprocesos por núcleo predeterminados: 2
- vCPU predeterminadas: 16 (8 * 2)
- Número válido de núcleos de CPU: 2, 4, 6, 8
- Número válido de subprocesos por núcleo: 1, 2

Deshabilitar el multiproceso

Para deshabilitar el multiproceso, especifique 1 subproceso por núcleo.

New console

Deshabilitación del multiproceso durante la inicialización de una instancia

1. Siga el procedimiento inicialización rápido de una instancia y configure la instancia según sea necesario.
2. Expanda Detalles avanzados y active la casilla Especificar opciones de CPU.
3. Para Core count (Número de núcleos), elija el número de núcleos de CPU necesarios. En este ejemplo, para especificar el número de núcleos de CPU predeterminado para una instancia `r5.4xlarge`, elija 8.
4. Para deshabilitar el multiproceso para Threads per core (Subprocesos por núcleo), elija 1.
5. En el panel Summary (Resumen), revise la configuración de la instancia y, a continuación, elija Launch instance (iniciar instancia). Para obtener más información, consulte Lance una instancia con el nuevo asistente de inicialización de instancias.

Old console

Deshabilitación del multiproceso durante la inicialización de una instancia

1. Siga el procedimiento indicado en Lance una instancia con el antiguo asistente de inicialización de instancias.
2. En la página Configure Instance Details (Configurar detalles de instancia), para CPU options (Opciones de CPU), elija Specify CPU options (Especificar opciones de CPU).
3. Para Core count (Número de núcleos), elija el número de núcleos de CPU necesarios. En este ejemplo, para especificar el número de núcleos de CPU predeterminado para una instancia `r5.4xlarge`, elija 8.
4. Para deshabilitar el multiproceso para Threads per core (Subprocesos por núcleo), elija 1.
5. Continúe tal y como se lo indique el asistente. Cuando haya acabado de revisar las opciones de la página Review Instance Launch (Revisar inicialización de instancia), elija Launch (iniciar). Para obtener más información, consulte Lance una instancia con el antiguo asistente de inicialización de instancias.

AWS CLI

Deshabilitación del multiproceso durante la inicialización de una instancia

Utilice el comando run-instances de la AWS CLI y especifique un valor de 1 para `ThreadsPerCore` en el parámetro `--cpu-options`. En `CoreCount`, especifique el número de núcleos de CPU. En este ejemplo, para especificar el número de núcleos de CPU predeterminado para una instancia `r5.4xlarge`, especifique un valor para 8.

```
aws ec2 run-instances \
    --image-id ami-1a2b3c4d \
    --instance-type r5.4xlarge \
    --cpu-options "CoreCount=8,ThreadsPerCore=1" \
    --key-name MyKeyPair
```

Especificar un número personalizado de vCPU en la inicialización

Puede personalizar el número de núcleos de CPU y subprocesos por núcleo para la instancia.

En el siguiente ejemplo se inicia una instancia `r5.4xlarge` con 4 vCPU.

New console

Especificación de un número personalizado de CPU virtuales durante la inicialización de una instancia

1. Siga el procedimiento inicialización rápido de una instancia y configure la instancia según sea necesario.
2. Expanda Detalles avanzados y active la casilla Especificar opciones de CPU.
3. Para obtener 4 vCPU, especifique 2 núcleos de CPU y 2 subprocesos por núcleo, como se indica a continuación:
   - En Número de núcleos, elija 2.
   - Para Threads per core (Subprocesos por núcleo), elija 2.
4. En el panel Summary (Resumen), revise la configuración de la instancia y, a continuación, elija Launch instance (iniciar instancia). Para obtener más información, consulte Lance una instancia con el nuevo asistente de inicialización de instancias.

Old console

Especificación de un número personalizado de CPU virtuales durante la inicialización de una instancia

1. Siga el procedimiento indicado en Lance una instancia con el antiguo asistente de inicialización de instancias.
2. En la página Configure Instance Details (Configurar detalles de instancia), para CPU options (Opciones de CPU), elija Specify CPU options (Especificar opciones de CPU).
3. Para obtener 4 vCPU, especifique 2 núcleos de CPU y 2 subprocesos por núcleo, como se indica a continuación:
   - En Número de núcleos, elija 2.
   - Para Threads per core (Subprocesos por núcleo), elija 2.
4. Continúe tal y como se lo indique el asistente. Cuando haya acabado de revisar las opciones de la página Review Instance Launch (Revisar inicialización de instancia), elija Launch (iniciar). Para obtener más información, consulte Lance una instancia con el antiguo asistente de inicialización de instancias.

AWS CLI

Especificación de un número personalizado de CPU virtuales durante la inicialización de una instancia

Utilice el comando run-instances de la AWS CLI y especifique el número de núcleos de CPU y el número de subprocesos en el parámetro `--cpu-options`. Puede especificar 2 núcleos de CPU y 2 subprocesos por núcleo para obtener 4 vCPU.

```
aws ec2 run-instances \
    --image-id ami-1a2b3c4d \
    --instance-type r5.4xlarge \
    --cpu-options "CoreCount=2,ThreadsPerCore=2" \
    --key-name MyKeyPair
```

También puede especificar 4 núcleos de CPU y 1 subproceso por núcleo (lo que deshabilita el multiproceso) para obtener 4 vCPU:

```
aws ec2 run-instances \
    --image-id ami-1a2b3c4d \
```

```
    --instance-type r5.4xlarge \
    --cpu-options "CoreCount=4,ThreadsPerCore=1" \
    --key-name MyKeyPair
```

Especificación de un número personalizado de vCPU en la plantilla de inicialización

Puede personalizar el número de núcleos de CPU y subprocesos por núcleo para la instancia en una plantilla de inicialización.

En el siguiente ejemplo se crea una plantilla de inicialización que especifica la configuración de una instancia `r5.4xlarge` con 4 vCPU.

Console

Para especificar un número personalizado de vCPU en la plantilla de inicialización

1. Siga el procedimiento Creación de una plantilla de inicialización a partir de parámetros y configure la plantilla de inicialización según sea necesario.
2. Expanda Detalles avanzados y active la casilla Especificar opciones de CPU.
3. Para obtener 4 vCPU, especifique 2 núcleos de CPU y 2 subprocesos por núcleo, como se indica a continuación:
   - En Número de núcleos, elija 2.
   - Para Threads per core (Subprocesos por núcleo), elija 2.
4. En el panel Resumen, revise la configuración de la instancia y, a continuación, elija Crear plantilla de inicialización. Para obtener más información, consulte iniciar una instancia desde una plantilla de inicialización.

AWS CLI

Para especificar un número personalizado de vCPU en la plantilla de inicialización

Utilice el comando de AWS CLI create-launch-template y especifique el número de núcleos de CPU y el número de subprocesos en el parámetro `CpuOptions`. Puede especificar 2 núcleos de CPU y 2 subprocesos por núcleo para obtener 4 vCPU.

```
aws ec2 create-launch-template \
    --launch-template-name TemplateForCPUOptions \
    --version-description CPUOptionsVersion1 \
```

```
    --launch-template-data file://template-data.json
```

A continuación se muestra un archivo JSON de ejemplo que contiene los datos de la plantilla de inicialización, entre los que se incluye las opciones de CPU, de la configuración de la instancia de este ejemplo.

```
{
    "NetworkInterfaces": [{
        "AssociatePublicIpAddress": true,
        "DeviceIndex": 0,
        "Ipv6AddressCount": 1,
        "SubnetId": "subnet-7b16de0c"
    }],
    "ImageId": "ami-8c1be5f6",
    "InstanceType": "r5.4xlarge",
    "TagSpecifications": [{
        "ResourceType": "instance",
        "Tags": [{
            "Key":"Name",
            "Value":"webserver"
        }]
    }],
    "CpuOptions": {
        "CoreCount":2,
        "ThreadsPerCore":2
    }
}
```

También puede especificar 4 núcleos de CPU y 1 subproceso por núcleo (lo que deshabilita el multiproceso) para obtener 4 vCPU:

```
{
    "NetworkInterfaces": [{
        "AssociatePublicIpAddress": true,
        "DeviceIndex": 0,
        "Ipv6AddressCount": 1,
        "SubnetId": "subnet-7b16de0c"
    }],
    "ImageId": "ami-8c1be5f6",
    "InstanceType": "r5.4xlarge",
    "TagSpecifications": [{
        "ResourceType": "instance",
```

```
        "Tags": [{
            "Key":"Name",
            "Value":"webserver"
        }]
    }],
    "CpuOptions": {
        "CoreCount":4,
        "ThreadsPerCore":1
    }
}
```

Visualizar las opciones de CPU de una instancia

Puede ver las opciones de CPU de una instancia existente en la consola de Amazon EC2 o describiendo la instancia mediante la AWS CLI.

Console

Para ver las opciones de CPU de una instancia utilizando la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación izquierdo, elija Instances (instancia[s]) y seleccione la instancia.
3. En la pestaña Details (Detalles), en Host and placement group (Host y grupo de ubicación), busque Number of vCPUs (Número de CPU virtuales).

AWS CLI

Para ver las opciones de CPU para una instancia (AWS CLI)

Utilice el comando describe-instances.

```
aws ec2 describe-instances --instance-ids i-123456789abcde123
```

```
...
    "Instances": [
        {
            "Monitoring": {
                "State": "disabled"
            },
            "PublicDnsName": "ec2-198-51-100-5.eu-central-1.compute.amazonaws.com",
```

```
            "State": {
                "Code": 16,
                "Name": "running"
            },
            "EbsOptimized": false,
            "LaunchTime": "2018-05-08T13:40:33.000Z",
            "PublicIpAddress": "198.51.100.5",
            "PrivateIpAddress": "172.31.2.206",
            "ProductCodes": [],
            "VpcId": "vpc-1a2b3c4d",
            "CpuOptions": {
                "CoreCount": 34,
                "ThreadsPerCore": 1
            },
            "StateTransitionReason": "",
            ...
        }
    ]
...
```

En la respuesta obtenida, el campo `CoreCount` indica el número de núcleos de la instancia. El campo `ThreadsPerCore` indica el número de subprocesos por núcleo.

Como alternativa, para ver la información de la CPU, puede conectarse a su instancia y usar una de las siguientes herramientas del sistema:

- Windows `Task Manager` en su instancia de Windows
- El comando lscpu de la instancia de Linux

Puede usar AWS Config para registrar, auditar y evaluar los cambios en la configuración de las instancias, incluidas las instancias terminadas. Para obtener más información, consulte Introducción a AWS Config en la AWS ConfigGuía para desarrolladores.

SEV-SNP de AMD en Amazon EC2

La virtualización cifrada segura y la paginación anidada segura de AMD (SEV-SNP de AMD) es una característica de la CPU que proporciona las siguientes propiedades:

- Atestación: la SEV-SNP de AMD le permite recuperar un informe de atestación firmado que contiene una medida criptográfica que se puede utilizar para validar el estado y la identidad de la

instancia, y que se ejecuta en hardware original de AMD. Para obtener más información, consulte Atestación con SEV-SNP de AMD.

- Cifrado de memoria: a partir de los procesadores AMD EPYC (Milan), AWS Graviton2 e Intel Xeon Scalable (Ice Lake), la memoria de instancias siempre está cifrada. Las instancias que están habilitadas para la SEV-SNP de AMD utilizan una clave específica de la instancia para el cifrado de la memoria.

Conceptos y terminología

Antes de empezar a utilizar la SEV-SNP de AMD, asegúrese de conocer los siguientes conceptos y terminología:

Informe de certificación de SEV-SNP de AMD

El informe de atestación de SEV-SNP de AMD es un documento que una instancia puede solicitar a la CPU. El informe de atestación de SEV-SNP de AMD se puede utilizar para validar el estado y la identidad de una instancia y para comprobar que se ejecuta en un entorno de AMD autorizado. El informe incluye una medición de inicialización, que es un hash criptográfico del estado de arranque inicial de una instancia, incluido el contenido de la memoria de la instancia inicial y el estado inicial de las CPU virtuales. El informe de atestación de SEV-SNP de AMD está firmado con una firma VLEK que se remonta a una raíz de confianza de AMD.

VLEK

La clave de aprobación cargada y versionada (VLEK) es una clave de firma versionada certificada por AMD. La utiliza la CPU de AMD para firmar los informes de atestación de SEV-SNP de AMD. Las firmas VLEK se pueden validar mediante certificados proporcionados por AMD.

OVMF binario

El firmware de máquina virtual abierta (OVMF) es el código de arranque anticipado que se utiliza para proporcionar un entorno UEFI para la instancia. El código de arranque anticipado se ejecuta antes de que se inicie el código de la AMI. El OVMF también busca y ejecuta el gestor de arranque que se proporciona en la AMI. Para obtener más información, consulte el Repositorio de OVMF.

Requisitos

Para utilizar la SEV-SNP de AMD, debe hacer lo siguiente:

- Utilice uno de los siguientes tipos de instancia admitidos:

  - De uso general: `m6a.large` | `m6a.xlarge` | `m6a.2xlarge` | `m6a.4xlarge` | `m6a.8xlarge`
  - Optimizadas para la computación: `c6a.large` | `c6a.xlarge` | `c6a.2xlarge` | `c6a.4xlarge` | `c6a.8xlarge` | `c6a.12xlarge` | `c6a.16xlarge`
  - Optimizadas para memoria: `r6a.large` | `r6a.xlarge` | `r6a.2xlarge` | `r6a.4xlarge`
- Lance su instancia en una Región de AWS compatible. Actualmente, solo se admiten Este de EE. UU. (Ohio) y Europa (Irlanda).
- Utilice una AMI con modo de arranque `uefi` o `uefi-preferred` y un sistema operativo compatible con la SEV-SNP de AMD. Para obtener más información sobre la compatibilidad con la SEV-SNP de AMD en su sistema operativo, consulte la documentación del sistema operativo correspondiente. En el caso de AWS, la SEV-SNP de AMD es compatible con AL2023, RHEL 9.3, SLES 15 SP4 y Ubuntu 23.04 y versiones posteriores.

Consideraciones

Sólo se puede activar SEV-SNP de AMD cuando se inicializa una instancia. Cuando la SEV-SNP de AMD esté activada para la inicialización de la instancia, se aplicarán las siguientes reglas.

- No se puede desactivar la SEV-SNP de AMD. Permanece activada durante todo el ciclo de vida de la instancia.
- Sólo puede cambiar el tipo de instancia por otro que admita SEV-SNP de AMD.
- No se admiten Hibernation ni Nitro Enclaves.
- No se admiten los hosts dedicados.
- Si el host subyacente de su instancia está programado para mantenimiento, recibirá una notificación de evento programado 14 días antes del evento. Debe detener o reiniciar la instancia manualmente para moverla a un nuevo host.

Precios

Al iniciar una instancia de Amazon EC2 con la característica SEV-SNP de AMD activada, se le cobrará una tarifa de uso por hora adicional que equivale al 10 por ciento de la tarifa horaria bajo demanda del tipo de instancia seleccionado.

Esta tarifa de uso de la SEV-SNP de AMD es un cargo independiente del uso de la instancia de Amazon EC2. Las instancias reservadas, Savings Plans y el uso del sistema operativo no afectan a esta tarifa.

Si configura una instancia de spot para iniciarla con la característica SEV-SNP de AMD activada, se le cobrará una tarifa de uso por hora adicional que equivale al 10 por ciento de la tarifa horaria bajo demanda del tipo de instancia seleccionado. Si la estrategia de asignación utiliza el precio como entrada, la flota de spot no incluye esta tarifa adicional; solo se utiliza el precio de spot.

Trabajo con SEV-SNP de AMD en Amazon EC2

Realice las siguientes tareas para trabajar con SEV-SNP de AMD en Amazon EC2.

Tareas

- Búsqueda de los tipos de instancia admitidos.
- Activación de la SEV-SNP de AMD en la inicialización
- Comprobación del estado de la SEV-SNP de AMD

Búsqueda de los tipos de instancia admitidos.

Puede utilizar la AWS CLI para buscar tipos de instancias compatibles con la SEV-SNP de AMD.

Para buscar los tipos de instancia compatibles con la SEV-SNP de AMD con la AWS CLI, utilice el siguiente comando describe-instance-types:

```
$ C:\> aws ec2 describe-instance-types \
--filters Name=processor-info.supported-features,Values=amd-sev-snp \
--query 'InstanceTypes[*].InstanceType'
```

Resultado de ejemplo.

```
[
 "r6a.2xlarge",
 "m6a.large",
 "m6a.2xlarge",
 "r6a.xlarge",
 "c6a.16xlarge",
 "c6a.8xlarge",
 "m6a.4xlarge",
 "c6a.12xlarge",
 "r6a.4xlarge",
 "c6a.xlarge",
 "c6a.4xlarge",
 "c6a.2xlarge",
 "m6a.xlarge",
```

```
 "c6a.large",
 "r6a.large",
 "m6a.8xlarge"
]
```

Activación de la SEV-SNP de AMD en la inicialización

Puede usar la AWS CLI para iniciar una instancia con la SEV-SNP de AMD activada.

Para iniciar una instancia con la SEV-SNP de AMD activada mediante la AWS CLI, utilice el comando run-instances e incluya la opción `--cpu-options AmdSevSnp=enabled`. En el caso de `--image-id`, especifique una AMI con el modo de arranque `uefi` o `uefi-prefered` y un sistema operativo compatible con la SEV-SNP de AMD. En el caso de `--instance-type`, especifique un tipo de instancia compatible.

```
$ C:\> aws ec2 run-instances \
--image-id supported_ami_id \
--instance-type supported_instance_type \
--key-name key_pair_name \
--subnet-id subnet_id \
--cpu-options AmdSevSnp=enabled
```

Comprobación del estado de la SEV-SNP de AMD

Puede utilizar uno de los métodos siguientes para comprobar el estado del SEV-SNP de AMD.

AWS CLI

Para comprobar si la SEV-SNP de AMD está activada en una instancia con la AWS CLI, utilice el comando describe-instances. En el caso de `--instance-ids`, especifique el ID de la instancia que desea comprobar.

```
$ C:\> aws ec2 describe-instances --instance-ids instance_id
```

En la salida del comando, el valor de `AmdSevSnp` en `CpuOptions` indica si la SEV-SNP de AMD está activada o desactivada.

AWS CloudTrail

En el evento de AWS CloudTrail para la solicitud de inicialización de la instancia, el valor `"cpuOptions": {"AmdSevSnp": enabled}` indica que la SEV-SNP de AMD está activada para la instancia.

Atestación con SEV-SNP de AMD

La atestación es un proceso que permite que la instancia demuestre su estado e identidad. Cuando activa la SEV-SNP de para su instancia, puede solicitar un informe de atestación de SEV-SNP de AMD al procesador subyacente. El informe de atestación de SEV-SNP de AMD contiene un hash criptográfico, denominado medición de inicialización, del contenido inicial de la memoria huésped y del estado inicial de la CPU virtual. El informe de atestación está firmado con una firma VLEK que se remonta a una raíz de confianza de AMD. Puede usar la medición de inicialización incluida en el informe de atestación para validar que la instancia se ejecuta en un entorno de AMD genuino y validar el código de arranque inicial que se usó para iniciar la instancia.

Complete los siguientes pasos para realizar la atestación con la SEV-SNP de AMD.

Paso 1: obtenga el informe de atestación

En este paso, instalará y compilará la utilidad `snpguest` y, a continuación, la usará para solicitar el informe de atestación de SEV-SNP de AMD y los certificados.

1. Ejecute los siguientes comandos para crear la utilidad `snpguest` desde el snpguest repository.

   ```
   $ C:\> git clone https://github.com/virtee/snpguest.git
   $ C:\> cd snpguest
   $ C:\> cargo build -r
   $ C:\> cd target/release
   ```

2. Genera una solicitud para el informe de certificación. La utilidad solicita el informe de certificación al host y lo escribe en un archivo binario con los datos de solicitud proporcionados.

   En el siguiente ejemplo, se crea una cadena de solicitud aleatoria y se utiliza como archivo de solicitud ()`request-file.txt`. Cuando el comando devuelve el informe de certificación, se almacena en la ruta del archivo que especifiques ()`report.bin`. En este caso, la utilidad guarda el informe en el directorio actual.

   ```
   $ C:\> ./snpguest report report.bin request-file.txt --random
   ```

3. Solicite los certificados de la memoria del host y guárdelos como archivos PEM. El siguiente ejemplo almacena los archivos en el mismo directorio que la `snpguest` utilidad. Si los certificados ya existen en el directorio especificado, se sobrescriben.

   ```
   $ C:\> ./snpguest certificates PEM ./
   ```

Paso 2: valide la firma del informe de atestación

El informe de atestación se firma con un certificado, denominado clave de aprobación cargada y versionada (VLEK), emitido por AMD para AWS. En este paso, puede validar que AMD haya emitido el certificado VLEK y que el informe de atestación esté firmado por dicho certificado.

1. Descargue los certificados raíz de confianza de VLEK del sitio web oficial de AMD en el directorio actual.

```
$ C:\> sudo curl --proto '=https' --tlsv1.2 -sSf https://kdsintf.amd.com/vlek/v1/
Milan/cert_chain -o ./cert_chain.pem
```

2. Utilice `openssl` para validar que el certificado VLEK esté firmado por los certificados raíz de confianza de AMD.

```
$ C:\> sudo openssl verify --CAfile ./cert_chain.pem vlek.pem
```

   Resultado previsto:

```
certs/vcek.pem: OK
```

3. Debe usar la utilidad `snpguest` para validar que el informe de atestación esté firmado por el certificado VLEK.

```
$ C:\> ./snpguest verify attestation ./ report.bin
```

   Resultado previsto.

```
Reported TCB Boot Loader from certificate matches the attestation report.
Reported TCB TEE from certificate matches the attestation report.
Reported TCB SNP from certificate matches the attestation report.
Reported TCB Microcode from certificate matches the attestation report.
VEK signed the Attestation Report!
```

Agregado de componentes de Windows a través de medios de instalación

Los sistemas operativos de Windows Server incluyen muchos componentes opcionales. Incluir todos los componentes opcionales en cada AMI de Windows Server de Amazon EC2 no es práctico. En

su lugar, le proporcionamos instantáneas de EBS de medios de instalación que tienen los archivos necesarios para configurar o instalar componentes en la instancia de Windows.

Para obtener acceso e instalar los componentes opcionales, primero debe encontrar la instantánea de EBS correcta para la versión de Windows Server, crear un volumen desde la instantánea y adjuntar el volumen a la instancia.

Antes de empezar

Utilice la AWS Management Console o una herramienta de línea de comandos para obtener el ID y la zona de disponibilidad de la instancia. Debe crear el volumen de EBS en la misma zona de disponibilidad que la instancia.

Agregar componentes de Windows mediante la consola

Use el siguiente procedimiento para añadir componentes de Windows a la instancia mediante la AWS Management Console.

Para añadir componentes de Windows a una instancia mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Snapshots (Instantáneas).
3. En la barra Filter (Filtro), elija Public Snapshots (Instantáneas públicas).
4. Agregue el filtro Owner Alias (Alias del propietario) y elija amazon.
5. Agregue el filtro Description (Descripción) e introduzca **`Windows`**.
6. Pulse Enter (Intro).
7. Seleccione la instantánea que coincida con la arquitectura del sistema y la preferencia de idioma. Por ejemplo, seleccione Medios de instalación de Windows 2019 en inglés si la instancia está ejecutando Windows Server 2019.
8. Elija Actions (Acciones), Create volume from snapshots (Crear volumen a partir de instantáneas).
9. En Availability Zone (Zona de disponibilidad), seleccione la zona de disponibilidad que corresponda a la instancia de Windows. Elija Add tag (Agregar etiqueta) e ingrese **`Name`** para la clave de la etiqueta y un nombre descriptivo para el valor de la etiqueta. Seleccione Create volume (Crear volumen).
10. En el mensaje Successfully created volume (El volumen se ha creado correctamente) (banner verde), elija el volumen que acaba de crear.

11. Elija Actions (Acciones), Attach Volume (Adjuntar volumen).
12. Desde Instance (instancia), seleccione el ID de la instancia.
13. Para Device Name (Nombre del dispositivo), introduzca el nombre del dispositivo para el archivo adjunto. Si necesita ayuda con el nombre del dispositivo, consulte Nombres de dispositivos en las instancias de Amazon EC2.
14. Elija Attach volume (Asociar volumen).
15. Conéctese a la instancia y haga que el volumen esté disponible. Para obtener más información, consulte Cómo hacer que un volumen de Amazon EBS esté disponible para su uso en la Guía del usuario de Amazon EBS.

> **Important**
>
> No inicialice el volumen.

16. Abra el Panel de control, Programas y características. Elija Activar o desactivar las características de Windows. Si se le solicitan los medios de instalación, especifique el volumen de EBS con los medios de instalación.
17. (Opcional) Cuando haya terminado de utilizar el medio de instalación, puede desconectar el volumen. Una vez desconectado el volumen, puede eliminarlo.

Agregar componentes de Windows mediante Tools for Windows PowerShell

Use el siguiente procedimiento para añadir componentes de Windows a la instancia mediante la Tools for Windows PowerShell.

Agregado de componentes de Windows a la instancia mediante Tools for Windows PowerShell

1. Use el cmdlet Get-EC2Snapshot con los filtros `Owner` y `description` para obtener una lista de las instantáneas de medios de instalación disponibles.

```
PS C:\> Get-EC2Snapshot -Owner amazon -Filter @{ Name="description";
 Values="Windows*" }
```

2. En los resultados, anote el ID de la instantánea que coincida con la arquitectura del sistema y la preferencia de idioma. Por ejemplo:

```
...
```

```
DataEncryptionKeyId :
Description         : Windows 2019 English Installation Media
Encrypted           : False
KmsKeyId            :
OwnerAlias          : amazon
OwnerId             : 123456789012
Progress            : 100%
SnapshotId          : snap-22da283e
StartTime           : 10/25/2019 8:00:47 PM
State               : completed
StateMessage        :
Tags                : {}
VolumeId            : vol-be5eafcb
VolumeSize          : 6
...
```

3. Use el cmdlet New-EC2Volume para crear un volumen a partir de la instantánea. Especifique la misma zona de disponibilidad que la de la instancia.

```
PS C:\> New-EC2Volume -AvailabilityZone us-east-1a -VolumeType gp2 -
SnapshotId snap-22da283e
```

4. En los resultados, anote el ID de volumen.

```
Attachments      : {}
AvailabilityZone : us-east-1a
CreateTime       : 4/18/2017 10:50:25 AM
Encrypted        : False
Iops             : 100
KmsKeyId         :
Size             : 6
SnapshotId       : snap-22da283e
State            : creating
Tags             : {}
VolumeId         : vol-06aa9e1fbf8b82ed1
VolumeType       : gp2
```

5. Use el cmdlet Add-EC2Volume para asociar el volumen a la instancia.

```
PS C:\> Add-EC2Volume -InstanceId i-087711ddaf98f9489 -
VolumeId vol-06aa9e1fbf8b82ed1 -Device xvdh
```

6. Conéctese a la instancia y haga que el volumen esté disponible. Para obtener más información, consulte Cómo hacer que un volumen de Amazon EBS esté disponible para su uso en la Guía del usuario de Amazon EBS.

   > **Important**
   >
   > No inicialice el volumen.

7. Abra el Panel de control, Programas y características. Elija Activar o desactivar las características de Windows. Si se le solicitan los medios de instalación, especifique el volumen de EBS con los medios de instalación.
8. (Opcional) Cuando haya terminado con los medios de instalación, utilice el cmdlet Dismount-EC2Volume para desconectar el volumen de la instancia. Una vez desconectado el volumen, puede utilizar el cmdlet Remove-EC2Volume para eliminarlo.

Agregar componentes de Windows mediante AWS CLI

Use el siguiente procedimiento para añadir componentes de Windows a la instancia mediante la AWS CLI.

Para añadir componentes de Windows a la instancia mediante la AWS CLI

1. Use el comando describe-snapshots con el parámetro `owner-ids` y el filtro `description` para obtener una lista de las instantáneas de medios de instalación disponibles.

```
aws ec2 describe-snapshots --owner-ids amazon --filters
 Name=description,Values=Windows*
```

2. En los resultados, anote el ID de la instantánea que coincida con la arquitectura del sistema y la preferencia de idioma. Por ejemplo:

```
{
    "Snapshots": [
    ...
        {
            "OwnerAlias": "amazon",
            "Description": "Windows 2019 English Installation Media",
            "Encrypted": false,
            "VolumeId": "vol-be5eafcb",
            "State": "completed",
```

```
            "VolumeSize": 6,
            "Progress": "100%",
            "StartTime": "2019-10-25T20:00:47.000Z",
            "SnapshotId": "snap-22da283e",
            "OwnerId": "123456789012"
        },
    ...
    ]
}
```

3. Use el comando create-volume para crear un volumen a partir de la instantánea. Especifique la misma zona de disponibilidad que la de la instancia.

```
aws ec2 create-volume --snapshot-id snap-22da283e --volume-type gp2 --availability-
zone us-east-1a
```

4. En los resultados, anote el ID de volumen.

```
{
    "AvailabilityZone": "us-east-1a",
    "Encrypted": false,
    "VolumeType": "gp2",
    "VolumeId": "vol-0c98b37f30bcbc290",
    "State": "creating",
    "Iops": 100,
    "SnapshotId": "snap-22da283e",
    "CreateTime": "2017-04-18T10:33:10.940Z",
    "Size": 6
}
```

5. Use el comando attach-volume para asociar el volumen a la instancia.

```
aws ec2 attach-volume --volume-id vol-0c98b37f30bcbc290 --instance-
id i-01474ef662b89480 --device xvdg
```

6. Conéctese a la instancia y haga que el volumen esté disponible. Para obtener más información, consulte Cómo hacer que un volumen de Amazon EBS esté disponible para su uso en la Guía del usuario de Amazon EBS.

> **Important**
>
> No inicialice el volumen.

7. Abra el Panel de control, Programas y características. Elija Activar o desactivar las características de Windows. Si se le solicitan los medios de instalación, especifique el volumen de EBS con los medios de instalación.
8. (Opcional) Cuando haya terminado con los medios de instalación, utilice el comando detach-volume para desconectar el volumen de la instancia. Una vez desconectado el volumen, puede utilizar el comando delete-volume para eliminarlo.

Administración de usuarios del sistema en la instancia de Linux

Cada de instancia de Linux se inicia con un usuario predeterminado del sistema Linux. Puede agregar usuarios a la instancia y eliminarlos.

En el caso del usuario predeterminado, la AMI determina el nombre de usuario predeterminado que se especificó cuando lanzó la instancia.

> **Note**
>
> De forma predeterminada, la autenticación con contraseña y el inicio de sesión raíz están desactivados y sudo está habilitado. Para iniciar sesión en la instancia, debe usar un par de claves. Para obtener más información acerca del formato del archivo de registro, consulte Conexión con la instancia de Linux.
> Puede permitir la autenticación con contraseña y el inicio de sesión raíz para la instancia. Para obtener más información, consulte la documentación del sistema operativo.

> **Note**
>
> Los usuarios del sistema Linux no deben confundirse con los usuarios de IAM. Para obtener más información, consulte Usuarios de IAM en la Guía del usuario de IAM.

Contenido

Nombres de usuario predeterminados

La AMI determina el nombre de usuario predeterminado que se especificó cuando lanzó la instancia.

Los nombres de usuario predeterminados son:

- Para AL2023, Amazon Linux 2 o la AMI de Amazon Linux, el nombre de usuario es `ec2-user`.
- Para una AMI de CentOS, el nombre de usuario es `centos` o `ec2-user`.
- Para una AMI de Debian, el nombre de usuario es `admin`.
- Para una AMI de Fedora, el nombre de usuario es `fedora` o `ec2-user`.
- Para una AMI de RHEL, el nombre de usuario es `ec2-user` o `root`.
- Para una AMI de SUSE, el nombre de usuario es `ec2-user` o `root`.
- Para una AMI de Ubuntu, el nombre de usuario es `ubuntu`.
- Para una AMI de Oracle, el nombre de usuario es `ec2-user`.
- Para una AMI de Bitnami, el nombre de usuario es `bitnami`.

> **Note**
>
> Para encontrar el nombre de usuario predeterminado para otras distribuciones de Linux, consulte con el proveedor de AMI.

Consideraciones

Es correcto utilizar lel usuario predeterminado para muchas aplicaciones. Sin embargo, es posible que elija agregar usuarios de modo que las personas puedan tener sus propios archivos y zonas de trabajo. Además, crear usuarios para usuarios nuevos es mucho más seguro que conceder a múltiples usuarios (posiblemente inexpertos) acceso al usuario predeterminado porque el usuario predeterminado puede causar mucho daño en un sistema si no se usa adecuadamente. Para obtener más información, consulte Sugerencias para proteger la instancia de EC2.

Para permitir a los usuarios el acceso SSH a su instancia de EC2 mediante un usuario del sistema Linux, debe compartir la clave SSH con el usuario. De forma alternativa, puede utilizar EC2 Instance Connect para permitir el acceso a los usuarios sin necesidad de compartir y administrar claves SSH. Para obtener más información, consulte Conéctese a la instancia de Linux con EC2 Instance Connect.

Creación de un usuario

En primer lugar, cree el usuario y, a continuación, agregue la clave pública SSH que permite al usuario conectar e iniciar sesión en la instancia.

Creación de un usuario

1. Cree un nuevo par de claves. Debe proporcionar el archivo `.pem` al usuario para el que va a crearlo. Debe usar este archivo para conectarse a la instancia.
2. Recupere la clave pública del par de claves que creó en el paso anterior.

   ```
   $ C:\>  ssh-keygen -y -f /path_to_key_pair/key-pair-name.pem
   ```

   El comando devuelve la clave pública, como se muestra en el siguiente ejemplo.

   ```
   ssh-rsa
    AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6Vhz2ItxCih
   +PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/
   d6RJhJOI0iBXrlsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/
   i8SeJtjnV3iAoG/cQk+0FzZqaeJAAHco
   +CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi
   +z7wB3RbBQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE
   ```

3. Conéctese a la instancia.
4. Utilice el comando adduser para crear el usuario y añádala al sistema (con una entrada en el archivo `/etc/passwd`). El comando también crea un grupo y un directorio principal para el usuario. En este ejemplo, el usuario se denomina *newuser*.

   - Amazon Linux y Amazon Linux 2

     Con Amazon Linux y Amazon Linux 2, el usuario se crea con la autenticación por contraseña inhabilitada por defecto.

```
[ec2-user ~]$ sudo adduser newuser
```

- Ubuntu

  Incluya el parámetro `--disabled-password` para crear el usuario con la autenticación con contraseña desactivada.

```
[ubuntu ~]$ sudo adduser newuser --disabled-password
```

5. Cambie al nuevo usuario de forma que el directorio y el archivo que cree tengan la propiedad adecuada.

```
[ec2-user ~]$ sudo su - newuser
```

   El símbolo cambia de `ec2-user` a *`newuser`* para indicar que ha transferido la sesión del shell al nuevo usuario.

6. Agregar la clave pública SSH al usuario. En primer lugar, cree un directorio en el directorio de inicio del usuario para el archivo de clave SSH, a continuación cree el archivo de clave y, finalmente, pegue la clave pública en el archivo de clave, tal como se describe en los siguientes pasos secundarios.

   a. Cree un directorio `.ssh` en el directorio principal *`newuser`* y cambie los permisos de archivo a `700` (solo el propietario puede leer, escribir o abrir el directorio).

```
[newuser ~]$ mkdir .ssh
```

```
[newuser ~]$ chmod 700 .ssh
```

> **Important**
>
> Sin estos permisos de archivo exactos, el usuario no podrá iniciar sesión.

   b. Cree un archivo llamado `authorized_keys` en el directorio `.ssh` y cambie los permisos de archivo a `600` (solo el propietario puede leer o escribir en el archivo).

```
[newuser ~]$ touch .ssh/authorized_keys
```

```
[newuser ~]$ chmod 600 .ssh/authorized_keys
```

> **Important**
>
> Sin estos permisos de archivo exactos, el usuario no podrá iniciar sesión.

c. Abra el archivo `authorized_keys` con el editor de texto que prefiera (como vim o nano).

```
[newuser ~]$ nano .ssh/authorized_keys
```

Pegue la clave pública que recuperó en el paso 2 en el archivo y guarde los cambios.

> **Important**
>
> Asegúrese de pegar la clave pública en una línea continua. La clave pública no debe dividirse en varias líneas.

Ahora el usuario debería poder iniciar sesión en el usuario *`newuser`* de la instancia usando la clave privada que corresponde a la clave pública que ha agregado al archivo `authorized_keys`. Para obtener más información acerca de los diferentes métodos de conexión a una instancia de Linux, consulte Conexión con la instancia de Linux.

Eliminación de un usuario

Si ya no necesita un usuario, puede eliminarlo para que no pueda volver a utilizarse.

Utilice el comando userdel para eliminar el usuario del sistema. Cuando especifica el parámetro `-r`, el directorio principal del usuario y la carpeta spool de correo se eliminan. Para mantener el directorio principal del usuario y la carpeta spool de correo, omita el parámetro `-r`.

```
[ec2-user ~]$ sudo userdel -r olduser
```

Establecer la contraseña del administrador de Windows para su instancia

Cuando se conecta a una instancia de Windows, debe especificar una cuenta de usuario y una contraseña que tenga permiso de acceso a la instancia. La primera vez que se conecta a una instancia, se le pide que especifique la cuenta de administrador y la contraseña predeterminadas.

Con las AMI de Windows de AWS para Windows Server 2012 R2 y versiones anteriores, Configuración de una instancia de Windows mediante el servicio EC2Config (heredado) genera la contraseña predeterminada. Con las AMI de Windows de AWS para Windows Server 2016 y 2019, Configurar una instancia de Windows utilizando EC2Launch genera la contraseña predeterminada. Con las AMI de Windows de AWS para Windows Server 2022 y versiones posteriores, Configurar una instancia de Windows mediante EC2Launch v2 genera la contraseña predeterminada.

> **Note**
>
> Con Windows Server 2016 y versiones anteriores, la opción `Password never expires` está deshabilitada para el administrador local. Con Windows Server 2012 R2 y versiones anteriores, la opción `Password never expires` está habilitada para el administrador local.

Cambiar la contraseña de administrador tras la conexión

Cuando se conecta a una instancia por primera vez, recomendamos que cambie la contraseña de administrador de su valor predeterminado. Use el procedimiento siguiente para cambiar la contraseña de administrador para una instancia de Windows.

> **Important**
>
> Guarde la nueva contraseña en un lugar seguro. No podrá recuperar la nueva contraseña utilizando la consola de Amazon EC2. La consola solo puede recuperar la contraseña predeterminada. Si intenta conectarse a la instancia con la contraseña predeterminada después de cambiarla, recibirá un error "Your credentials did not work".

Para cambiar la contraseña del administrador local

1. Conéctese a la instancia y abra un símbolo del sistema.
2. Ejecute el siguiente comando. Si la contraseña nueva incluye caracteres especiales, asegúrese de incluirla entre comillas dobles.

```
net user Administrator "new_password"
```

3. Guarde la nueva contraseña en un lugar seguro.

Cambiar una contraseña perdida o caducada

Si pierde la contraseña o esta vence, puede generar una nueva. Para conocer los procedimientos para restablecer la contraseña, consulte Restablecer una contraseña de administrador de Windows perdida o vencida.

Administrar controladores de dispositivos para su instancia de Amazon EC2

Algunos controladores no vienen preinstalados en la AMI de EC2 desde la que se inicia. Es posible que otros necesiten actualizaciones para aprovechar la funcionalidad ampliada. Los siguientes temas tratan sobre la instalación, las actualizaciones y la configuración de algunos de los controladores de dispositivos que están conectados a las instancias EC2.

Contenido

Instalación de controladores NVIDIA en su instancia de Amazon EC2

Una instancia con una GPU NVIDIA asociada, como una instancia P3 o G4dn, debe tener instalado el controlador NVIDIA apropiado. En función del tipo de instancias, puede descargar un controlador público de NVIDIA, descargar un controlador de Amazon S3 que está disponible solo para clientes de AWS o utilizar una AMI con el controlador preinstalado.

Para instalar controladores AMD en una instancia con una GPU AMD asociada, como una instancia G4ad, consulte Instalar controladores AMD. Para instalar los controladores NVIDIA, consulte Instalación de controladores NVIDIA.

Contenido

Tipos de controladores NVIDIA

Los siguientes son los principales tipos de controladores NVIDIA que se pueden usar con instancias basadas en GPU.

Controladores Tesla

Estos controladores están destinados principalmente a cargas de trabajo informáticas, que utilizan GPU para tareas computacionales como cálculos de punto flotante paralelos para machine learning y transformadas rápidas de Fourier para aplicaciones informáticas de alto rendimiento.

Controladores GRID

Estos controladores están certificados para proporcionar un rendimiento óptimo para aplicaciones de visualización profesionales que procesan contenido tales como modelos 3D o vídeos de alta resolución. Puede configurar los controladores GRID para que admitan dos modos. Las estaciones de trabajo virtuales Quadro proporcionan acceso a cuatro pantallas 4K por GPU. Las vApps GRID proporcionan capacidades de alojamiento de aplicaciones RDSH.

Controladores de juegos

Estos controladores contienen optimizaciones para juegos y se actualizan con frecuencia para proporcionar mejoras de rendimiento. Son compatibles con una sola pantalla 4K por GPU.

Modo configurado

En Windows, los controladores Tesla están configurados para ejecutarse en el modo Tesla Compute Cluster (TCC). Los controladores GRID y de juegos están configurados para ejecutarse en el

modo Modelo de controlador de pantalla de Windows (WDDM). En el modo TCC, la tarjeta está dedicada a calcular cargas de trabajo. En el modo WDDM, la tarjeta admite cargas de trabajo tanto de computación como de gráficos.

Panel de control de NVIDIA

El panel de control de NVIDIA es compatible con los controladores GRID y Gaming. No es compatible con los controladores Tesla.

API compatibles para Tesla, GRID y controladores de juegos

- OpenCL, OpenGL y Vulkan
- NVIDIA CUDA y bibliotecas relacionadas (por ejemplo, cuDNN, TensorRT, nvJPEG y cuBLAS)
- NVENC para la codificación de vídeo y NVDEC para la decodificación de vídeo
- API sólo para Windows: DirectX, Direct2D, DirectX Video Acceleration, DirectX Raytracing

Controladores disponibles por tipo de instancia

En la siguiente tabla se resumen los controladores NVIDIA admitidos para cada tipo de instancia de GPU.

Tipo de instancia	Controlador Tesla	Controlador GRID	Controlador de juegos
G3	Sí	Sí	No
G4dn	Sí	Sí	Sí
G5	Sí	Sí	Sí
G5g	Sí[1]	No	No
G6	Sí	Sí	No
Gr6	Sí	Sí	No
P2	Sí	No	No
P3	Sí	No	No
P4d	Sí	No	No

Tipo de instancia	Controlador Tesla	Controlador GRID	Controlador de juegos
P4de	Sí	No	No

[1] Este controlador Tesla también admite aplicaciones gráficas optimizadas específicas de la plataforma ARM64

[2] Utilizando solo AMI de Marketplace

Opciones de instalación

Utilice una de las siguientes opciones para obtener los controladores NVIDIA necesarios para su instancia de GPU.

Opciones

- Opción 1: las AMI con los controladores NVIDIA instalados
- Opción 2: controladores públicos de NVIDIA
- Opción 3: controladores GRID (instancias G6, Gr6, G5, G4dn y G3)
- Opción 4: controladores de videojuegos NVIDIA (instancias G5 y G4dn)

Opción 1: las AMI con los controladores NVIDIA instalados

AWS y NVIDIA ofrecen distintas Imágenes de máquina de Amazon (AMI) que vienen con los controladores NVIDIA instalados.

- Ofertas de Marketplace con el controlador Tesla
- Ofertas de Marketplace con el controlador GRID
- Ofertas de Marketplace con el controlador de juegos

Para revisar las consideraciones que dependen de la plataforma de su sistema operativo (SO), elija la pestaña que corresponda a su AMI.

Linux

> Para actualizar la versión del controlador instalada con una de estas AMI, debe desinstalar los paquetes NVIDIA de su instancia para evitar conflictos de versiones. Utilice este comando para desinstalar los paquetes NVIDIA:

```
[ec2-user ~]$ sudo yum erase nvidia cuda
```

El paquete de conjunto de herramientas CUDA tiene dependencias en los controladores de NVIDIA. Al desinstalar los paquetes de NVIDIA se borra el conjunto de herramientas CUDA. Debe volver a instalar el conjunto de herramientas CUDA tras instalar el controlador de NVIDIA.

Windows

Si crea una AMI de Windows personalizada con una de las ofertas de AWS Marketplace, la AMI debe ser una imagen estandarizada creada con Windows Sysprep para garantizar que el controlador GRID funcione. Para obtener más información, consulte Creación de una AMI con Windows Sysprep.

Opción 2: controladores públicos de NVIDIA

Las opciones ofrecidas por AWS incluyen la licencia necesaria para el controlador. Como opción, puede instalar los controladores públicos y traer su propia licencia. Para instalar un controlador público, descárguelo desde el sitio NVIDIA como se describe aquí.

Como opción, puede utilizar las opciones ofrecidas por AWS en lugar de los controladores públicos. Para utilizar un controlador GRID en una instancia P3, utilice las AMI de AWS Marketplace como se describe en la Opción 1. Para utilizar un controlador GRID en una instancia G6, Gr6, G5, G4dn o G3, utilice las AWS Marketplace AMI como se describe en la Opción 1 o instale los controladores NVIDIA proporcionados por AWS como se describe en Opción 3: controladores GRID (instancias G6, Gr6, G5, G4dn y G3).

Para descargar un controlador público de NVIDIA

Inicie sesión en su instancia y descargue el controlador NVIDIA de 64 bits adecuado para el tipo de instancia http://www.nvidia.com/Download/Find.aspx. En Tipo de producto, Serie de producto y Producto, utilice las opciones de la tabla siguiente.

instancia	Tipo de producto	Serie de producto	Producto
G3	Tesla	Clase M	M60
G4dn	Tesla	Serie T	T4
G5[1]	Tesla	Serie A	A10

instancia	Tipo de producto	Serie de producto	Producto
G5g[2]	Tesla	Serie T	NVIDIA T4G
G6 [3]	Tesla	Serie L	L4
Gr6 [3]	Tesla	Serie L	L4
P2	Tesla	Serie K	K80
P3	Tesla	Serie V	V100
P4d	Tesla	Serie A	A100
P4de	Tesla	Serie A	A100
P5[4]	Tesla	Serie H	H100

[1] Las instancias G5 requieren la versión 470.00 del controlador o posterior.

[2] Las instancias G5g requieren la versión 470.82.01 del controlador o posterior. El sistema operativo es Linux aarch64.

[3] Las instancias G6 y Gr6 requieren la versión del controlador 525.0 o posterior.

[4] Las instancias P5 requieren la versión de controlador 530 o posterior.

Para instalar el controlador NVIDIA en sistemas operativos Linux, consulte la Guía de inicio rápido para la instalación de controladores NVIDIA.

Para instalar el controlador NVIDIA en Windows, siga estos pasos:

1. Abra la carpeta donde ha descargado el controlador y lance el archivo de instalación. Siga las instrucciones para instalar el controlador y reiniciar la instancia como sea necesario.
2. Deshabilite el adaptador de pantalla denominado Adaptador de pantalla básico de Microsoft que está marcado con un icono de advertencia mediante el Administrador de dispositivos. Instale estas características de Windows: Media Foundation y Quality Windows Audio Video Experience.

> **Important**
>
> No deshabilite el adaptador de pantalla denominado Adaptador de pantalla remoto de Microsoft. Si el Adaptador de pantalla remoto de Microsoft está deshabilitado, la conexión podría interrumpirse y los intentos de conectarse a la instancia después de reiniciarla podrían fallar.

3. Compruebe el Administrador de dispositivos para verificar que la GPU está funcionando correctamente.
4. Para obtener el mejor rendimiento de su GPU, realice los pasos de optimización que se indican en Optimización de las configuraciones de GPU en instancias de Amazon EC2.

Opción 3: controladores GRID (instancias G6, Gr6, G5, G4dn y G3)

Estas descargas solo están disponibles para los clientes de AWS. Al realizar la descarga, con el fin de cumplir los requisitos de la AWS solución mencionados en el Acuerdo de Licencia de Usuario Final (EULA) de NVIDIA GRID Cloud, usted acepta utilizar el software descargado únicamente para desarrollar AMIs para su uso con el hardware NVIDIA L4, NVIDIA A10G, NVIDIA Tesla T4 o NVIDIA Tesla M60. Al instalar el software, estará sujeto a los términos del Contrato de licencia para el usuario final de NVIDIA GRID Cloud. Para obtener información sobre la versión del controlador NVIDIA GRID para su sistema operativo, consulte la documentación del software NVIDIA® Virtual GPU (vGPU) en el sitio web de NVIDIA.

Consideraciones

- Las instancias G6 y Gr6 requieren GRID 17 o una versión posterior.
- Las instancias G5 requieren GRID 13.1 o posterior (o GRID 12.4 o posterior).
- Las instancias G3 necesitan la resolución de DNS que proporciona AWS para que las licencias de GRID funcionen.
- IMDSv2 solo es compatible con el controlador NVIDIA versión 14.0 o las versiones posteriores.
- Para instancias de Windows, si inicializa su instancia desde una AMI de Windows personalizada, la AMI debe ser una imagen estandarizada creada usando Windows Sysprep para asegurarse de que el driver GRID funciona. Para obtener más información, consulte Creación de una AMI con Windows Sysprep.
- Las versiones 17.0 y posteriores de GRID no son compatibles con Windows Server 2019.

- Las versiones 14.2 y posteriores de GRID no son compatibles con Windows Server 2016.
- Las instancias G3 no admiten GRID 17.0 y versiones posteriores.

Amazon Linux y Amazon Linux 2

Para instalar el controlador GRID de NVIDIA en su instancia

1. Conexión con la instancia de Linux.
2. Instale la AWS CLI en su instancia de Linux y configure las credenciales predeterminadas. Para obtener más información, consulte Instalación de AWS CLI en la Guía del usuario de AWS Command Line Interface.

   > **Important**
   >
   > Su usuario o rol deben tener los permisos concedidos que contiene la política AmazonS3ReadOnlyAccess. Para obtener más información, consulte la política administrada de AWS: AmazonS3ReadOnlyAccess en la Guía del usuario de Amazon Simple Storage Service.

3. Instale gcc y make, si aún no están instalados.

   ```
   [ec2-user ~]$ sudo yum install gcc make
   ```

4. Actualice la caché del paquete y obtenga las actualizaciones del paquete para la instancia.

   ```
   [ec2-user ~]$ sudo yum update -y
   ```

5. Reinicie la instancia para cargar la última versión de kernel.

   ```
   [ec2-user ~]$ sudo reboot
   ```

6. Vuelva a conectarse a su instancia una vez que se haya reiniciado.
7. Instale el compilador de gcc y el paquete de encabezados del kernel para la versión del kernel que está ejecutando actualmente.

   ```
   [ec2-user ~]$ sudo yum install -y gcc kernel-devel-$(uname -r)
   ```

8. Descargue la utilidad de instalación del controlador GRID mediante el siguiente comando:

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

En este bucket se almacenan varias versiones del controlador GRID. Puede ver todas las versiones disponibles mediante el comando siguiente:

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

9. Añada permisos para ejecutar la utilidad de instalación del controlador mediante el comando siguiente.

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

10. Ejecute el script de autoinstalación de la siguiente manera para instalar el controlador GRID que descargó. Por ejemplo:

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

> **Note**
>
> Si utiliza Amazon Linux 2 con kernel, versión 5.10, utilice el comando siguiente para instalar el controlador GRID.
>
> ```
> [ec2-user ~]$ sudo CC=/usr/bin/gcc10-cc ./NVIDIA-Linux-x86_64*.run
> ```

Cuando se le pregunte, acepte el contrato de licencia y especifique las opciones de instalación según sea necesario (puede aceptar las opciones predeterminadas).

11. Confirme que el controlador está funcionando. La respuesta del siguiente comando indica la versión de controlador de NVIDIA instalado y los detalles de las GPU.

```
[ec2-user ~]$ nvidia-smi -q | head
```

12. Si utiliza la versión 14.x o superior del software de la GPU virtual de NVIDIA en las instancias G4dn, G5 o G5g, deshabilite GSP con los siguientes comandos. Para obtener más información sobre por qué es necesario, consulte la documentación de NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/modprobe.d/nvidia.conf
```

13. Reinicie la instancia.

```
[ec2-user ~]$ sudo reboot
```

14. (Opcional) En función de su caso de uso, es posible que tenga que completar los siguientes pasos opcionales. Si no necesita esta funcionalidad, no complete estos pasos.

    a. Para poder aprovechar las cuatro pantallas de resolución de hasta 4K, configure el protocolo de pantalla de alto rendimiento NICE DCV.

    b. El modo NVIDIA Quadro Virtual Workstation está habilitado de forma predeterminada. Para activar las aplicaciones virtuales de GRID para capacidades de alojamiento de aplicaciones RDSH, complete los pasos para activar aplicaciones virtuales de GRID en Activación de las aplicaciones virtuales NVIDIA GRID en las instancias de Amazon EC2 basadas en GPU.

CentOS 7 y Red Hat Enterprise Linux 7

Para instalar el controlador GRID de NVIDIA en su instancia

1. Conexión con la instancia de Linux. Instale gcc y make, si aún no están instalados.
2. Actualice la caché del paquete y obtenga las actualizaciones del paquete para la instancia.

```
[ec2-user ~]$ sudo yum update -y
```

3. Reinicie la instancia para cargar la última versión de kernel.

```
[ec2-user ~]$ sudo reboot
```

4. Vuelva a conectarse a su instancia una vez que se haya reiniciado.
5. Instale el compilador de gcc y el paquete de encabezados del kernel para la versión del kernel que está ejecutando actualmente.

```
[ec2-user ~]$ sudo yum install -y gcc kernel-devel-$(uname -r)
```

6. Deshabilite el controlador de código abierto `nouveau` para tarjetas gráficas NVIDIA.

   a. Añada `nouveau` al archivo de lista de no admitidos de `/etc/modprobe.d/blacklist.conf`. Copie el siguiente bloque de código y péguelo en un terminal.

   ```
   [ec2-user ~]$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
   blacklist vga16fb
   blacklist nouveau
   blacklist rivafb
   blacklist nvidiafb
   blacklist rivatv
   EOF
   ```

   b. Edite el archivo `/etc/default/grub` y añada la línea siguiente:

   ```
   GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
   ```

   c. Reconstruya la configuración de Grub.

   ```
   [ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
   ```

7. Descargue la utilidad de instalación del controlador GRID mediante el siguiente comando:

   ```
   [ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
   ```

   En este bucket se almacenan varias versiones del controlador GRID. Puede ver todas las versiones disponibles mediante el comando siguiente:

   ```
   [ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
   ```

8. Añada permisos para ejecutar la utilidad de instalación del controlador mediante el comando siguiente.

   ```
   [ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
   ```

9. Ejecute el script de autoinstalación de la siguiente manera para instalar el controlador GRID que descargó. Por ejemplo:

   ```
   [ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
   ```

Cuando se le pregunte, acepte el contrato de licencia y especifique las opciones de instalación según sea necesario (puede aceptar las opciones predeterminadas).

10. Confirme que el controlador está funcionando. La respuesta del siguiente comando indica la versión de controlador de NVIDIA instalado y los detalles de las GPU.

```
[ec2-user ~]$ nvidia-smi -q | head
```

11. Si utiliza la versión 14.x o superior del software de la GPU virtual de NVIDIA en las instancias G4dn, G5 o G5g, deshabilite GSP con los siguientes comandos. Para obtener más información sobre por qué es necesario, consulte la documentación de NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

12. Reinicie la instancia.

```
[ec2-user ~]$ sudo reboot
```

13. (Opcional) En función de su caso de uso, es posible que tenga que completar los siguientes pasos opcionales. Si no necesita esta funcionalidad, no complete estos pasos.

    a. Para poder aprovechar las cuatro pantallas de resolución de hasta 4K, configure el protocolo de pantalla de alto rendimiento NICE DCV.

    b. El modo NVIDIA Quadro Virtual Workstation está habilitado de forma predeterminada. Para activar las aplicaciones virtuales de GRID para capacidades de alojamiento de aplicaciones RDSH, complete los pasos para activar aplicaciones virtuales de GRID en Activación de las aplicaciones virtuales NVIDIA GRID en las instancias de Amazon EC2 basadas en GPU.

    c. Instale el paquete de escritorio/estación de trabajo GUI.

```
[ec2-user ~]$ sudo yum groupinstall -y "Server with GUI"
```

CentOS Stream 8 y Red Hat Enterprise Linux 8

Para instalar el controlador GRID de NVIDIA en su instancia

1. Conexión con la instancia de Linux. Instale gcc y make, si aún no están instalados.
2. Actualice la caché del paquete y obtenga las actualizaciones del paquete para la instancia.

```
[ec2-user ~]$ sudo yum update -y
```

3. Reinicie la instancia para cargar la última versión de kernel.

```
[ec2-user ~]$ sudo reboot
```

4. Vuelva a conectarse a su instancia una vez que se haya reiniciado.
5. Instale el compilador de gcc y el paquete de encabezados del kernel para la versión del kernel que está ejecutando actualmente.

```
[ec2-user ~]$ sudo dnf install -y make gcc elfutils-libelf-devel libglvnd-devel
 kernel-devel-$(uname -r)
```

6. Descargue la utilidad de instalación del controlador GRID mediante el siguiente comando:

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

   En este bucket se almacenan varias versiones del controlador GRID. Puede ver todas las versiones disponibles mediante el comando siguiente:

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

7. Añada permisos para ejecutar la utilidad de instalación del controlador mediante el comando siguiente.

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

8. Ejecute el script de autoinstalación de la siguiente manera para instalar el controlador GRID que descargó. Por ejemplo:

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

Cuando se le pregunte, acepte el contrato de licencia y especifique las opciones de instalación según sea necesario (puede aceptar las opciones predeterminadas).

9. Confirme que el controlador está funcionando. La respuesta del siguiente comando indica la versión de controlador de NVIDIA instalado y los detalles de las GPU.

```
[ec2-user ~]$ nvidia-smi -q | head
```

10. Si utiliza la versión 14.x o superior del software de la GPU virtual de NVIDIA en las instancias G4dn, G5 o G5g, deshabilite GSP con los siguientes comandos. Para obtener más información sobre por qué es necesario, consulte la documentación de NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

11. Reinicie la instancia.

```
[ec2-user ~]$ sudo reboot
```

12. (Opcional) En función de su caso de uso, es posible que tenga que completar los siguientes pasos opcionales. Si no necesita esta funcionalidad, no complete estos pasos.

    a. Para poder aprovechar las cuatro pantallas de resolución de hasta 4K, configure el protocolo de pantalla de alto rendimiento NICE DCV.

    b. El modo NVIDIA Quadro Virtual Workstation está habilitado de forma predeterminada. Para activar las aplicaciones virtuales de GRID para capacidades de alojamiento de aplicaciones RDSH, complete los pasos para activar aplicaciones virtuales de GRID en Activación de las aplicaciones virtuales NVIDIA GRID en las instancias de Amazon EC2 basadas en GPU.

    c. Instale el paquete de estación de trabajo GUI.

```
[ec2-user ~]$ sudo dnf groupinstall -y workstation
```

Rocky Linux 8

Para instalar el controlador NVIDIA GRID en su instancia de Linux

1. Conexión con la instancia de Linux. Instale gcc y make, si aún no están instalados.
2. Actualice la caché del paquete y obtenga las actualizaciones del paquete para la instancia.

```
[ec2-user ~]$ sudo yum update -y
```

3. Reinicie la instancia para cargar la última versión de kernel.

```
[ec2-user ~]$ sudo reboot
```

4. Vuelva a conectarse a su instancia una vez que se haya reiniciado.
5. Instale el compilador de gcc y el paquete de encabezados del kernel para la versión del kernel que está ejecutando actualmente.

```
[ec2-user ~]$ sudo dnf install -y make gcc elfutils-libelf-devel libglvnd-devel
 kernel-devel-$(uname -r)
```

6. Descargue la utilidad de instalación del controlador GRID mediante el siguiente comando:

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

   En este bucket se almacenan varias versiones del controlador GRID. Puede ver todas las versiones disponibles mediante el comando siguiente:

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

7. Añada permisos para ejecutar la utilidad de instalación del controlador mediante el comando siguiente.

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

8. Ejecute el script de autoinstalación de la siguiente manera para instalar el controlador GRID que descargó. Por ejemplo:

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

Cuando se le pregunte, acepte el contrato de licencia y especifique las opciones de instalación según sea necesario (puede aceptar las opciones predeterminadas).

9. Confirme que el controlador está funcionando. La respuesta del siguiente comando indica la versión de controlador de NVIDIA instalado y los detalles de las GPU.

```
[ec2-user ~]$ nvidia-smi -q | head
```

10. Si utiliza la versión 14.x o superior del software de la GPU virtual de NVIDIA en las instancias G4dn, G5 o G5g, deshabilite GSP con los siguientes comandos. Para obtener más información sobre por qué es necesario, consulte la documentación de NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

11. Reinicie la instancia.

```
[ec2-user ~]$ sudo reboot
```

12. (Opcional) En función de su caso de uso, es posible que tenga que completar los siguientes pasos opcionales. Si no necesita esta funcionalidad, no complete estos pasos.

    a. Para poder aprovechar las cuatro pantallas de resolución de hasta 4K, configure el protocolo de pantalla de alto rendimiento NICE DCV.

    b. El modo NVIDIA Quadro Virtual Workstation está habilitado de forma predeterminada. Para activar las aplicaciones virtuales de GRID para capacidades de alojamiento de aplicaciones RDSH, complete los pasos para activar aplicaciones virtuales de GRID en Activación de las aplicaciones virtuales NVIDIA GRID en las instancias de Amazon EC2 basadas en GPU.

Ubuntu y Debian

Para instalar el controlador GRID de NVIDIA en su instancia

1. Conexión con la instancia de Linux. Instale gcc y make, si aún no están instalados.
2. Actualice la caché del paquete y obtenga las actualizaciones del paquete para la instancia.

```
$ sudo apt-get update -y
```

3. (Ubuntu) Actualice el paquete de `linux-aws` para obtener la última versión.

```
$ sudo apt-get upgrade -y linux-aws
```

(Debian) Actualice el paquete para obtener la última versión.

```
$ sudo apt-get upgrade -y
```

4. Reinicie la instancia para cargar la última versión de kernel.

```
$ sudo reboot
```

5. Vuelva a conectarse a su instancia una vez que se haya reiniciado.
6. Instale el compilador de gcc y el paquete de encabezados del kernel para la versión del kernel que está ejecutando actualmente.

```
$ sudo apt-get install -y gcc make linux-headers-$(uname -r)
```

7. Deshabilite el controlador de código abierto `nouveau` para tarjetas gráficas NVIDIA.

   a. Añada `nouveau` al archivo de lista de no admitidos de `/etc/modprobe.d/blacklist.conf`. Copie el siguiente bloque de código y péguelo en un terminal.

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

   b. Edite el archivo `/etc/default/grub` y añada la línea siguiente:

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

   c. Reconstruya la configuración de Grub.

```
$ sudo update-grub
```

8. Descargue la utilidad de instalación del controlador GRID mediante el siguiente comando:

```
$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

   En este bucket se almacenan varias versiones del controlador GRID. Puede ver todas las versiones disponibles mediante el comando siguiente:

```
$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

9. Añada permisos para ejecutar la utilidad de instalación del controlador mediante el comando siguiente.

```
$ chmod +x NVIDIA-Linux-x86_64*.run
```

10. Ejecute el script de autoinstalación de la siguiente manera para instalar el controlador GRID que descargó. Por ejemplo:

```
$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

    Cuando se le pregunte, acepte el contrato de licencia y especifique las opciones de instalación según sea necesario (puede aceptar las opciones predeterminadas).

11. Confirme que el controlador está funcionando. La respuesta del siguiente comando indica la versión de controlador de NVIDIA instalado y los detalles de las GPU.

```
$ nvidia-smi -q | head
```

12. Si utiliza la versión 14.x o superior del software de la GPU virtual de NVIDIA en las instancias G4dn, G5 o G5g, deshabilite GSP con los siguientes comandos. Para obtener más información sobre por qué es necesario, consulte la documentación de NVIDIA.

```
$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/
modprobe.d/nvidia.conf
```

13. Reinicie la instancia.

```
$ sudo reboot
```

14. (Opcional) En función de su caso de uso, es posible que tenga que completar los siguientes pasos opcionales. Si no necesita esta funcionalidad, no complete estos pasos.

    a. Para poder aprovechar las cuatro pantallas de resolución de hasta 4K, configure el protocolo de pantalla de alto rendimiento NICE DCV.

    b. El modo NVIDIA Quadro Virtual Workstation está habilitado de forma predeterminada. Para activar las aplicaciones virtuales de GRID para capacidades de alojamiento de aplicaciones RDSH, complete los pasos para activar aplicaciones virtuales de GRID en Activación de las aplicaciones virtuales NVIDIA GRID en las instancias de Amazon EC2 basadas en GPU.

    c. Instale el paquete de escritorio/estación de trabajo GUI.

    ```
    $ sudo apt-get install -y lightdm ubuntu-desktop
    ```

Sistemas operativos Windows

Para instalar el controlador GRID de NVIDIA en la instancia de Windows

1. Conéctese a su instancia de Windows y abra una ventana de PowerShell.
2. Configure las credenciales predeterminadas para AWS Tools for Windows PowerShell en su instancia de Windows. Para obtener más información acerca de Cómo empezar a trabajar con AWS Tools for Windows PowerShell consulte la Guía del usuario de AWS Tools for Windows PowerShell.

    > **Important**
    >
    > Su usuario o rol deben tener los permisos concedidos que contiene la política AmazonS3ReadOnlyAccess. Para obtener más información, consulte la política administrada de AWS: AmazonS3ReadOnlyAccess en la Guía del usuario de Amazon Simple Storage Service.

3. Descargue los controladores y el contrato de licencia para el usuario final de NVIDIA GRID Cloud de Amazon S3 en su escritorio mediante los siguientes comandos de PowerShell.

    ```
    $Bucket = "ec2-windows-nvidia-drivers"
    $KeyPrefix = "latest"
    ```

```
$LocalPath = "$home\Desktop\NVIDIA"
$Objects = Get-S3Object -BucketName $Bucket -KeyPrefix $KeyPrefix -Region us-east-1
foreach ($Object in $Objects) {
$LocalFileName = $Object.Key
if ($LocalFileName -ne '' -and $Object.Size -ne 0) {
    $LocalFilePath = Join-Path $LocalPath $LocalFileName
    Copy-S3Object -BucketName $Bucket -Key $Object.Key -LocalFile $LocalFilePath -
Region us-east-1
}
}
```

En este bucket se almacenan varias versiones del controlador NVIDIA GRID. Puede descargar todas las versiones disponibles de Windows del bucket eliminando la opción `-KeyPrefix $KeyPrefix`. Para obtener información sobre la versión del controlador NVIDIA GRID para su sistema operativo, consulte la documentación del software NVIDIA® Virtual GPU (vGPU) en el sitio web de NVIDIA.

A partir de GRID versión 11.0, puede utilizar los controladores en `latest` para las instancias G3 y G4dn. No agregaremos versiones posteriores a la 11.0 a `g4/latest`, pero conservaremos la versión 11.0 y las versiones anteriores específicas de G4dn en `g4/latest`.

Las instancias G5 requieren GRID 13.1 o posterior (o GRID 12.4 o posterior).

4. Desplácese hasta el escritorio y haga doble clic en el archivo de instalación para iniciarlo (elija la versión de controlador que se corresponda con la versión del sistema operativo de la instancia). Siga las instrucciones para instalar el controlador y reiniciar la instancia como sea necesario. Para verificar que la GPU funciona correctamente, compruebe el administrador de dispositivos.
5. (Opcional) Use el comando siguiente para deshabilitar la página de licencia en el panel de control para evitar que los usuarios cambien accidentalmente el tipo de producto (el escritorio virtual de GRID de NVIDIA está habilitado de forma predeterminada). Para obtener más información, consulte la GRID Licensing User Guide.

   PowerShell

   Ejecute los siguientes comandos de PowerShell para crear el valor de registro a fin de deshabilitar la página de licencias en el panel de control. AWS Tools for PowerShell en las AMI de Windows de AWS es una versión de 32 bits y este comando devuelve un error. En su lugar, utilice la versión de 64 bits de PowerShell incluida con el sistema operativo.

   ```
   New-Item -Path "HKLM:\SOFTWARE\NVIDIA Corporation\Global" -Name GridLicensing
   ```

```
New-ItemProperty -Path "HKLM:\SOFTWARE\NVIDIA Corporation\Global\GridLicensing" -
Name "NvCplDisableManageLicensePage" -PropertyType "DWord" -Value "1"
```

Símbolo del sistema

Ejecute el comando de registro siguiente para crear el valor de registro a fin de deshabilitar la página de licencias en el panel de control. Puede ejecutarlo mediante la ventana Símbolo del sistema o una versión de 64 bits de PowerShell.

```
reg add "HKLM\SOFTWARE\NVIDIA Corporation\Global\GridLicensing" /v
 NvCplDisableManageLicensePage /t REG_DWORD /d 1
```

6. (Opcional) En función de su caso de uso, es posible que tenga que completar los siguientes pasos opcionales. Si no necesita esta funcionalidad, no complete estos pasos.

   a. Para poder aprovechar las cuatro pantallas de resolución de hasta 4K, configure el protocolo de pantalla de alto rendimiento, NICE DCV.

   b. El modo NVIDIA Quadro Virtual Workstation está habilitado de forma predeterminada. Para activar las aplicaciones virtuales de GRID para capacidades de alojamiento de aplicaciones RDSH, complete los pasos para activar aplicaciones virtuales de GRID en Activación de las aplicaciones virtuales NVIDIA GRID en las instancias de Amazon EC2 basadas en GPU.

Opción 4: controladores de videojuegos NVIDIA (instancias G5 y G4dn)

Estos controladores sólo están disponibles para los clientes de AWS. Al descargarlos, acepta que solo utilizará el software descargado para desarrollar AMI a fin de utilizarlas con el hardware NVIDIA A10G y Tesla T4 de NVIDIA. Al instalar el software, estará sujeto a los términos del Contrato de licencia para el usuario final de NVIDIA GRID Cloud.

Consideraciones

- Las instancias G3 necesitan la resolución de DNS que proporciona AWS para que las licencias de GRID funcionen.
- IMDSv2 solo es compatible con el controlador NVIDIA versión 495.x o las versiones posteriores.

Amazon Linux y Amazon Linux 2

Para instalar el controlador de videojuegos NVIDIA en su instancia

1. Conexión con la instancia de Linux.
2. Instale la AWS CLI en su instancia de Linux y configure las credenciales predeterminadas. Para obtener más información, consulte Instalación de AWS CLI en la Guía del usuario de AWS Command Line Interface.

   > **Important**
   >
   > Su usuario o rol deben tener los permisos concedidos que contiene la política AmazonS3ReadOnlyAccess. Para obtener más información, consulte la política administrada de AWS: AmazonS3ReadOnlyAccess en la Guía del usuario de Amazon Simple Storage Service.

3. Instale gcc y make, si aún no están instalados.

   ```
   [ec2-user ~]$ sudo yum install gcc make
   ```

4. Actualice la caché del paquete y obtenga las actualizaciones del paquete para la instancia.

   ```
   [ec2-user ~]$ sudo yum update -y
   ```

5. Reinicie la instancia para cargar la última versión de kernel.

   ```
   [ec2-user ~]$ sudo reboot
   ```

6. Vuelva a conectarse a su instancia una vez que se haya reiniciado.
7. Instale el compilador de gcc y el paquete de encabezados del kernel para la versión del kernel que está ejecutando actualmente.

   ```
   [ec2-user ~]$ sudo yum install -y gcc kernel-devel-$(uname -r)
   ```

8. Descargue la utilidad de instalación del controlador de juegos mediante el siguiente comando:

   ```
   [ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
   ```

En este bucket se almacenan varias versiones del controlador GRID de NVIDIA. Puede ver todas las versiones disponibles mediante el comando siguiente:

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

9. Extraiga la utilidad de instalación del controlador de juegos del archivo `.zip` descargado.

```
[ec2-user ~]$ unzip latest-driver-name.zip -d nvidia-drivers
```

10. Agregue permisos para ejecutar la utilidad de instalación del controlador mediante el comando siguiente:

```
[ec2-user ~]$ chmod +x nvidia-drivers/NVIDIA-Linux-x86_64*-grid.run
```

11. Ejecute el instalador mediante el siguiente comando:

```
[ec2-user ~]$ sudo ./nvidia-drivers/NVIDIA-Linux-x86_64*.run
```

> **Note**
>
> Si utiliza Amazon Linux 2 con kernel, versión 5.10, utilice el comando siguiente para instalar los controladores de videojuego de NVIDIA.
>
> ```
> [ec2-user ~]$ sudo CC=/usr/bin/gcc10-cc ./NVIDIA-Linux-x86_64*.run
> ```

Cuando se le pregunte, acepte el contrato de licencia y especifique las opciones de instalación según sea necesario (puede aceptar las opciones predeterminadas).

12. Utilice el siguiente comando para crear el archivo de configuración requerido.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

13. Utilice el siguiente comando para descargar el archivo de certificación y cambiar su nombre.

    - Para la versión 460.39 o posterior:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2023_9_22.cert"
```

- Para la versión 440.68 a 445.48:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
```

- Para versiones anteriores:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

14. Si está utilizando la versión 510.x o superior del controlador NVIDIA en las instancias G4dn, G5 o G5g, deshabilite GSP con los siguientes comandos. Para obtener más información sobre por qué es necesario, consulte la documentación de NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/modprobe.d/nvidia.conf
```

15. Reinicie la instancia.

```
[ec2-user ~]$ sudo reboot
```

16. (Opcional) Para utilizar la pantalla individual con resolución de hasta 4K, configure el protocolo de pantalla de alto rendimiento NICE DCV.

CentOS 7 y Red Hat Enterprise Linux 7

Para instalar el controlador de videojuegos NVIDIA en su instancia

1. Conexión con la instancia de Linux. Instale gcc y make, si aún no están instalados.
2. Actualice la caché del paquete y obtenga las actualizaciones del paquete para la instancia.

```
[ec2-user ~]$ sudo yum update -y
```

3. Reinicie la instancia para cargar la última versión de kernel.

```
[ec2-user ~]$ sudo reboot
```

4. Vuelva a conectarse a su instancia una vez que se haya reiniciado.
5. Instale el compilador de gcc y el paquete de encabezados del kernel para la versión del kernel que está ejecutando actualmente.

```
[ec2-user ~]$ sudo yum install -y unzip gcc kernel-devel-$(uname -r)
```

6. Deshabilite el controlador de código abierto `nouveau` para tarjetas gráficas NVIDIA.

   a. Añada `nouveau` al archivo de lista de no admitidos de `/etc/modprobe.d/blacklist.conf`. Copie el siguiente bloque de código y péguelo en un terminal.

   ```
   [ec2-user ~]$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
   blacklist vga16fb
   blacklist nouveau
   blacklist rivafb
   blacklist nvidiafb
   blacklist rivatv
   EOF
   ```

   b. Edite el archivo `/etc/default/grub` y añada la línea siguiente:

   ```
   GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
   ```

   c. Reconstruya la configuración de Grub.

   ```
   [ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
   ```

7. Descargue la utilidad de instalación del controlador de juegos mediante el siguiente comando:

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

   En este bucket se almacenan varias versiones del controlador GRID de NVIDIA. Puede ver todas las versiones disponibles mediante el comando siguiente:

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

8. Extraiga la utilidad de instalación del controlador de juegos del archivo `.zip` descargado.

```
[ec2-user ~]$ unzip vGPUSW-*vGaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

9. Agregue permisos para ejecutar la utilidad de instalación del controlador mediante el comando siguiente:

```
[ec2-user ~]$ chmod +x nvidia-drivers/Linux/NVIDIA-Linux-x86_64*-grid.run
```

10. Ejecute el instalador mediante el siguiente comando:

```
[ec2-user ~]$ sudo ./nvidia-drivers/Linux/NVIDIA-Linux-x86_64*.run
```

    Cuando se le pregunte, acepte el contrato de licencia y especifique las opciones de instalación según sea necesario (puede aceptar las opciones predeterminadas).

11. Utilice el siguiente comando para crear el archivo de configuración requerido.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

12. Utilice el siguiente comando para descargar el archivo de certificación y cambiar su nombre.

    - Para la versión 460.39 o posterior:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2023_9_22.cert"
```

    - Para la versión 440.68 a 445.48:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
```

    - Para versiones anteriores:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

13. Si está utilizando la versión 510.x o superior del controlador NVIDIA en las instancias G4dn, G5 o G5g, deshabilite GSP con los siguientes comandos. Para obtener más información sobre por qué es necesario, consulte la documentación de NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

14. Reinicie la instancia.

```
[ec2-user ~]$ sudo reboot
```

15. (Opcional) Para utilizar la pantalla individual con resolución de hasta 4K, configure el protocolo de pantalla de alto rendimiento NICE DCV. Si no necesita esta funcionalidad, no complete este paso.

CentOS Stream 8 y Red Hat Enterprise Linux 8

Para instalar el controlador de videojuegos NVIDIA en su instancia

1. Conexión con la instancia de Linux. Instale gcc y make, si aún no están instalados.
2. Actualice la caché del paquete y obtenga las actualizaciones del paquete para la instancia.

```
[ec2-user ~]$ sudo yum update -y
```

3. Reinicie la instancia para cargar la última versión de kernel.

```
[ec2-user ~]$ sudo reboot
```

4. Vuelva a conectarse a su instancia una vez que se haya reiniciado.
5. Instale el compilador de gcc y el paquete de encabezados del kernel para la versión del kernel que está ejecutando actualmente.

```
[ec2-user ~]$ sudo yum install -y unzip gcc kernel-devel-$(uname -r)
```

6. Descargue la utilidad de instalación del controlador de juegos mediante el siguiente comando:

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

En este bucket se almacenan varias versiones del controlador GRID de NVIDIA. Puede ver todas las versiones disponibles mediante el comando siguiente:

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

7. Extraiga la utilidad de instalación del controlador de juegos del archivo `.zip` descargado.

```
[ec2-user ~]$ unzip vGPUSW-*vGaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

8. Agregue permisos para ejecutar la utilidad de instalación del controlador mediante el comando siguiente:

```
[ec2-user ~]$ chmod +x nvidia-drivers/Linux/NVIDIA-Linux-x86_64*-grid.run
```

9. Ejecute el instalador mediante el siguiente comando:

```
[ec2-user ~]$ sudo ./nvidia-drivers/Linux/NVIDIA-Linux-x86_64*.run
```

   Cuando se le pregunte, acepte el contrato de licencia y especifique las opciones de instalación según sea necesario (puede aceptar las opciones predeterminadas).

10. Utilice el siguiente comando para crear el archivo de configuración requerido.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

11. Utilice el siguiente comando para descargar el archivo de certificación y cambiar su nombre.

    - Para la versión 460.39 o posterior:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2023_9_22.cert"
```

    - Para la versión 440.68 a 445.48:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
```

    - Para versiones anteriores:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

12. Si está utilizando la versión 510.x o superior del controlador NVIDIA en las instancias G4dn, G5 o G5g, deshabilite GSP con los siguientes comandos. Para obtener más información sobre por qué es necesario, consulte la documentación de NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/modprobe.d/nvidia.conf
```

13. Reinicie la instancia.

```
[ec2-user ~]$ sudo reboot
```

14. (Opcional) Para utilizar la pantalla individual con resolución de hasta 4K, configure el protocolo de pantalla de alto rendimiento NICE DCV.

Rocky Linux 8

Para instalar el controlador de videojuegos NVIDIA en su instancia

1. Conexión con la instancia de Linux. Instale gcc y make, si aún no están instalados.
2. Actualice la caché del paquete y obtenga las actualizaciones del paquete para la instancia.

```
[ec2-user ~]$ sudo yum update -y
```

3. Reinicie la instancia para cargar la última versión de kernel.

```
[ec2-user ~]$ sudo reboot
```

4. Vuelva a conectarse a su instancia una vez que se haya reiniciado.
5. Instale el compilador de gcc y el paquete de encabezados del kernel para la versión del kernel que está ejecutando actualmente.

```
[ec2-user ~]$ sudo dnf install -y unzip gcc make elfutils-libelf-devel libglvnd-devel kernel-devel-$(uname -r)
```

6. Descargue la utilidad de instalación del controlador de juegos mediante el siguiente comando:

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

En este bucket se almacenan varias versiones del controlador GRID de NVIDIA. Puede ver todas las versiones disponibles mediante el comando siguiente:

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

7. Extraiga la utilidad de instalación del controlador de juegos del archivo `.zip` descargado.

```
[ec2-user ~]$ unzip vGPUSW-*vGaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

8. Agregue permisos para ejecutar la utilidad de instalación del controlador mediante el comando siguiente:

```
[ec2-user ~]$ chmod +x nvidia-drivers/Linux/NVIDIA-Linux-x86_64*-grid.run
```

9. Ejecute el instalador mediante el siguiente comando:

```
[ec2-user ~]$ sudo ./nvidia-drivers/Linux/NVIDIA-Linux-x86_64*.run
```

Cuando se le pregunte, acepte el contrato de licencia y especifique las opciones de instalación según sea necesario (puede aceptar las opciones predeterminadas).

10. Utilice el siguiente comando para crear el archivo de configuración requerido.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

11. Utilice el siguiente comando para descargar el archivo de certificación y cambiar su nombre.
    - Para la versión 460.39 o posterior:

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2023_9_22.cert"
      ```

    - Para la versión 440.68 a 445.48:

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
      ```

    - Para versiones anteriores:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

12. Si está utilizando la versión 510.x o superior del controlador NVIDIA en las instancias G4dn, G5 o G5g, deshabilite GSP con los siguientes comandos. Para obtener más información sobre por qué es necesario, consulte la documentación de NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/modprobe.d/nvidia.conf
```

13. Reinicie la instancia.

```
[ec2-user ~]$ sudo reboot
```

14. (Opcional) Para utilizar la pantalla individual con resolución de hasta 4K, configure el protocolo de pantalla de alto rendimiento NICE DCV.

Ubuntu y Debian

Para instalar el controlador de videojuegos NVIDIA en su instancia

1. Conexión con la instancia de Linux. Instale gcc y make, si aún no están instalados.
2. Actualice la caché del paquete y obtenga las actualizaciones del paquete para la instancia.

```
$ sudo apt-get update -y
```

3. Actualice el paquete `linux-aws` para recibir la última versión.

```
$ sudo apt-get upgrade -y linux-aws
```

4. Reinicie la instancia para cargar la última versión de kernel.

```
$ sudo reboot
```

5. Vuelva a conectarse a su instancia una vez que se haya reiniciado.

6. Instale el compilador de gcc y el paquete de encabezados del kernel para la versión del kernel que está ejecutando actualmente.

```
$ sudo apt-get install -y unzip gcc make linux-headers-$(uname -r)
```

7. Deshabilite el controlador de código abierto `nouveau` para tarjetas gráficas NVIDIA.

   a. Añada `nouveau` al archivo de lista de no admitidos de `/etc/modprobe.d/blacklist.conf`. Copie el siguiente bloque de código y péguelo en un terminal.

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

   b. Edite el archivo `/etc/default/grub` y añada la línea siguiente:

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

   c. Reconstruya la configuración de Grub.

```
$ sudo update-grub
```

8. Descargue la utilidad de instalación del controlador de juegos mediante el siguiente comando:

```
$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

   En este bucket se almacenan varias versiones del controlador GRID de NVIDIA. Puede ver todas las versiones disponibles mediante el comando siguiente:

```
$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

9. Extraiga la utilidad de instalación del controlador de juegos del archivo `.zip` descargado.

```
$ unzip vGPUSW-*vGaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

10. Agregue permisos para ejecutar la utilidad de instalación del controlador mediante el comando siguiente:

```
$ chmod +x nvidia-drivers/Linux/NVIDIA-Linux-x86_64*-grid.run
```

11. Ejecute el instalador mediante el siguiente comando:

```
$ sudo ./nvidia-drivers/Linux/NVIDIA-Linux-x86_64*.run
```

Cuando se le pregunte, acepte el contrato de licencia y especifique las opciones de instalación según sea necesario (puede aceptar las opciones predeterminadas).

12. Utilice el siguiente comando para crear el archivo de configuración requerido.

```
$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

13. Utilice el siguiente comando para descargar el archivo de certificación y cambiar su nombre.
    - Para la versión 460.39 o posterior:

```
$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2023_9_22.cert"
```

    - Para la versión 440.68 a 445.48:

```
$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
```

    - Para versiones anteriores:

```
$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

14. Si está utilizando la versión 510.x o superior del controlador NVIDIA en las instancias G4dn, G5 o G5g, deshabilite GSP con los siguientes comandos. Para obtener más información sobre por qué es necesario, consulte la documentación de NVIDIA.

```
$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/
modprobe.d/nvidia.conf
```

15. Reinicie la instancia.

```
$ sudo reboot
```

16. (Opcional) Para utilizar la pantalla individual con resolución de hasta 4K, configure el protocolo de pantalla de alto rendimiento NICE DCV. Si no necesita esta funcionalidad, no complete este paso.

Sistemas operativos Windows

Antes de instalar un controlador NVIDIA para juegos en la instancia, debe asegurarse de que se cumplen los siguientes requisitos previos, además de las consideraciones mencionadas para todos los controladores de juegos.

- Si inicia la instancia de Windows con una AMI de Windows personalizada, la AMI debe ser una imagen estandarizada creada con Windows Sysprep para asegurarse de que el controlador de juego funciona. Para obtener más información, consulte Creación de una AMI con Windows Sysprep.
- Configure las credenciales predeterminadas para AWS Tools for Windows PowerShell en su instancia de Windows. Para obtener más información acerca de Cómo empezar a trabajar con AWS Tools for Windows PowerShell consulte la Guía del usuario de AWS Tools for Windows PowerShell.
- Sus usuarios o rol deben tener los permisos concedidos que contiene la política AmazonS3ReadOnlyAccess. Para obtener más información, consulte la política administrada de AWS: AmazonS3ReadOnlyAccess en la Guía del usuario de Amazon Simple Storage Service.

Para instalar el controlador de juegos NVIDIA en su instancia de Windows

1. Conéctese a su instancia de Windows y abra una ventana de PowerShell.
2. Descargue e instale el controlador de juegos mediante los siguientes comandos de PowerShell.

```
$Bucket = "nvidia-gaming"
$KeyPrefix = "windows/latest"
$LocalPath = "$home\Desktop\NVIDIA"
$Objects = Get-S3Object -BucketName $Bucket -KeyPrefix $KeyPrefix -Region us-east-1
foreach ($Object in $Objects) {
$LocalFileName = $Object.Key
if ($LocalFileName -ne '' -and $Object.Size -ne 0) {
```

```
    $LocalFilePath = Join-Path $LocalPath $LocalFileName
    Copy-S3Object -BucketName $Bucket -Key $Object.Key -LocalFile $LocalFilePath -
Region us-east-1
}
}
```

En este bucket de S3 se almacenan varias versiones del controlador GRID de NVIDIA. Puede descargar todas las versiones disponibles en el bucket si cambia el valor de la variable `$KeyPrefix` de “windows/latest” a “windows”.

3. Desplácese hasta el escritorio y haga doble clic en el archivo de instalación para iniciarlo (elija la versión de controlador que se corresponda con la versión del sistema operativo de la instancia). Siga las instrucciones para instalar el controlador y reiniciar la instancia como sea necesario. Para verificar que la GPU funciona correctamente, compruebe el Administrador de dispositivos.
4. Utilice uno de los siguientes métodos para registrar el controlador.

   Version 527.27 or above

   Cree la siguiente clave del registro con la versión de 64 bits de PowerShell o la ventana de símbolo del sistema.

   clave: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\nvlddmkm\Global`

   nombre: VGamingMarketplace

   tipo: DWord

   valor: 2

   PowerShell

   Ejecute el siguiente comando de PowerShell para crear este valor del registro. AWS Tools for PowerShell en las AMI de Windows de AWS es una versión de 32 bits y este comando devuelve un error. En su lugar, utilice la versión de 64 bits de PowerShell incluida con el sistema operativo.

   ```
   New-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\nvlddmkm\Global"
    -Name "vGamingMarketplace" -PropertyType "DWord" -Value "2"
   ```

   Símbolo del sistema

Ejecute el siguiente comando de registro para crear este valor de registro. Puede ejecutarlo mediante la ventana Símbolo del sistema o una versión de 64 bits de PowerShell.

```
reg add "HKLM\SYSTEM\CurrentControlSet\Services\nvlddmkm\Global" /v
 vGamingMarketplace /t REG_DWORD /d 2
```

Earlier versions

Cree la siguiente clave del registro con la versión de 64 bits de PowerShell o la ventana de símbolo del sistema.

clave: `HKEY_LOCAL_MACHINE\SOFTWARE\NVIDIA Corporation\Global`

nombre: VGamingMarketplace

tipo: DWord

valor: 2

PowerShell

Ejecute el siguiente comando de PowerShell para crear este valor del registro. AWS Tools for PowerShell en las AMI de Windows de AWS es una versión de 32 bits y este comando devuelve un error. En su lugar, utilice la versión de 64 bits de PowerShell incluida con el sistema operativo.

```
New-ItemProperty -Path "HKLM:\SOFTWARE\NVIDIA Corporation\Global" -Name
 "vGamingMarketplace" -PropertyType "DWord" -Value "2"
```

Símbolo del sistema

Ejecute el siguiente comando del registro para crear esta clave de registro con la ventana del símbolo del sistema. También puede utilizar este comando en la versión de 64 bits de PowerShell.

```
reg add "HKLM\SOFTWARE\NVIDIA Corporation\Global" /v vGamingMarketplace /t
 REG_DWORD /d 2
```

5. Ejecute el siguiente comando en PowerShell. Esto descarga el archivo de certificación, cambia el nombre del archivo a `GridSwCert.txt` y mueve el archivo a la carpeta de documentos

públicos de su unidad del sistema. Normalmente, la ruta de la carpeta es `C:\Users\Public\Documents`.

- Para la versión 461.40 o posterior:

```
Invoke-WebRequest -Uri "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertWindows_2023_9_22.cert" -OutFile "$Env:PUBLIC\Documents\GridSwCert.txt"
```

- Para la versión 445.87:

```
Invoke-WebRequest -Uri "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Windows_2020_04.cert" -OutFile "$Env:PUBLIC\Documents\GridSwCert.txt"
```

- Para versiones anteriores:

```
Invoke-WebRequest -Uri "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Windows_2019_09.cert" -OutFile "$Env:PUBLIC\Documents\GridSwCert.txt"
```

> **Note**
>
> Si recibe un error al descargar el archivo y está usando Windows Server 2016 o una versión anterior, es posible que sea necesario habilitar TLS 1.2 para su terminal PowerShell. Puede habilitar TLS 1.2 para la sesión actual de PowerShell con el siguiente comando y luego volver a intentarlo:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol =
>  [Net.SecurityProtocolType]::Tls12
> ```

6. Reinicie su instancia.
7. Verifique la licencia de NVIDIA Gaming mediante el siguiente comando.

```
C:\Windows\System32\DriverStore\FileRepository\nv_dispswi.inf_*\nvidia-smi.exe -q
```

El resultado debería ser similar al siguiente.

```
vGPU Software Licensed Product
```

```
Product Name                : NVIDIA Cloud Gaming
License Status              : Licensed (Expiry: N/A)
```

8. (Opcional) Para utilizar la pantalla individual de resolución de hasta 4K, configure el protocolo de pantalla de alto rendimiento NICE DCV. Si no necesita esta funcionalidad, no complete este paso.

Instalación de una versión adicional de CUDA

Después de instalar un controlador de gráficos NVIDIA en la instancia, puede instalar una versión de CUDA distinta de la versión incluida con el controlador de gráficos. El siguiente procedimiento muestra cómo configurar varias versiones de CUDA en la instancia.

Instalación del kit de herramientas CUDA en Linux

Siga estos pasos para instalar el kit de herramientas CUDA en Linux:

1. Conexión con la instancia de Linux.
2. Visite el sitio web de NVIDIA y seleccione la versión de CUDA que necesite.
3. Seleccione la arquitectura, la distribución y la versión del sistema operativo de su instancia. En Installer Type (Tipo de instalador), seleccione runfile (local).
4. Siga las instrucciones para descargar el script de instalación.
5. Agregue permisos de ejecución al script de instalación que ha descargado mediante el siguiente comando.

```
[ec2-user ~]$ chmod +x downloaded_installer_file
```

6. Ejecute el script de instalación de la siguiente forma para instalar el kit de herramientas CUDA y agregar el número de versión CUDA a la ruta del kit de herramientas.

```
[ec2-user ~]$ sudo sh downloaded_installer_file --silent --override --toolkit --
samples --toolkitpath=/usr/local/cuda-version --samplespath=/usr/local/cuda --no-
opengl-libs
```

7. (Opcional) Establezca la versión predeterminada de CUDA de la siguiente manera.

```
[ec2-user ~]$ sudo ln -s /usr/local/cuda-version /usr/local/cuda
```

Instalación del kit de herramientas CUDA en Windows

Siga estos pasos para instalar el kit de herramientas CUDA en Windows:

Para instalar el kit de herramientas CUDA

1. Conéctese a la instancia de Windows.
2. Visite el sitio web de NVIDIA y seleccione la versión de CUDA que necesite.
3. En Installer Type (Tipo de instalador), seleccione exe (local) y, a continuación, elija Download (Descargar).
4. Utilizando su navegador, ejecute el archivo de instalación descargado. Siga las instrucciones para instalar el kit de herramientas CUDA. Es posible que tenga que reiniciar la instancia.

Instalación de controladores AMD en su instancia de Amazon EC2

Una instancia con una GPU AMD conectada, como una instancia G4ad, debe tener instalado el controlador AMD adecuado. De acuerdo ami sus requisitos, puede usar una AMI con el controlador preinstalado o descargar un controlador desde Amazon S3.

Para instalar controladores NVIDIA en una instancia con una GPU NVIDIA conectada, como una instancia G4dn, consulte Instalación de controladores NVIDIA en su lugar.

Contenido

- Software AMD Radeon Pro para controladores empresariales
- AMI con el controlador AMD instalado
- Descargar controlador AMD
- Configuración de un escritorio interactivo para Linux

Software AMD Radeon Pro para controladores empresariales

El software AMD Radeon Pro para controladores empresariales está diseñado para ofrecer compatibilidad con los casos de uso de gráficos de nivel profesional. Con el controlador, puede configurar las instancias con dos pantallas 4K por GPU.

API compatibles:

- OpenGL, OpenCL

- Vulkan
- Marco multimedia avanzado de AMD
- API de aceleración de vídeo
- DirectX 9 y versiones posteriores
- Transformación de Microsoft Hardware Media Foundation

AMI con el controlador AMD instalado

AWS ofrece diferentes Imágenes de máquina de Amazon (AMI) que vienen con los controladores AMD instalados. Abra ofertas de Marketplace con el controlador AMD.

Descargar controlador AMD

Si no está utilizando una AMI con el controlador AMD instalado, puede descargar el controlador AMD e instalarlo en su instancia. Solo las siguientes versiones de los sistemas operativos admiten controladores AMD:

- Amazon Linux 2 con kernel versión 4.14

> **Note**
>
> La versión amdgpu-pro-20.20-1184451 del controlador AMD y las versiones más recientes requieren la versión 5.15 o superiores del kernel.

- Windows Server 2016
- Windows Server 2019

Estas descargas solo están disponibles para los clientes de AWS. Al descargarlo, acepta que solo utilizará el software descargado para desarrollar AMIs para utilizarlas con el hardware AMD Radeon Pro V520. Al instalar el software, estará sujeto a los términos del contrato de licencia para el usuario final de Software AMD.

Instalación del controlador AMD en su instancia de Linux

1. Conexión con la instancia de Linux.

2. Instale la AWS CLI en su instancia de Linux y configure las credenciales predeterminadas. Para obtener más información, consulte Instalación de AWS CLI en la Guía del usuario de AWS Command Line Interface.

   > **Important**
   >
   > Su usuario o rol deben tener los permisos concedidos que contiene la política AmazonS3ReadOnlyAccess. Para obtener más información, consulte la política administrada de AWS: AmazonS3ReadOnlyAccess en la Guía del usuario de Amazon Simple Storage Service.

3. Instale gcc y make, si aún no están instalados.

```
$ sudo yum install gcc make
```

4. Actualice la caché del paquete y obtenga las actualizaciones del paquete para la instancia.

   - En Amazon Linux 2:

```
$ sudo amazon-linux-extras install epel -y
$ sudo yum update -y
```

   - Para Ubuntu 22.04:

```
$ wget https://repo.radeon.com/.preview/a0e4ef1dffbc95b4abb54e891f265e61/amdgpu-install/5.5.02.05.2/ubuntu/jammy/amdgpu-install_5.5.02.05.50502-1_all.deb
$ sudo apt install ./amdgpu-install_5.5.02.05.50502-1_all.deb
$ sudo sed -i 's#repo.radeon.com#&/.preview/a0e4ef1dffbc95b4abb54e891f265e61#' /etc/apt/sources.list.d/{amdgpu.list,rocm.list,amdgpu-proprietary.list}
```

   - Para otras versiones de Ubuntu:

```
$ sudo dpkg --add-architecture i386
$ sudo apt-get update -y && sudo apt upgrade -y
```

   - Para CentOS:

```
$ sudo yum install epel-release -y
$ sudo yum update -y
```

5. Reinicie la instancia.

```
$ sudo reboot
```

6. Vuelva a conectar a la instancia después de que se reinicie.
7. Descargue el controlador AMD más reciente.

> **Note**
>
> Omite este paso para Ubuntu 22.04.

```
$ aws s3 cp --recursive s3://ec2-amd-linux-drivers/latest/ .
```

8. Extraiga el archivo.

   - Para Amazon Linux 2 y CentOS:

     ```
     $ tar -xf amdgpu-pro-*rhel*.tar.xz
     ```

   - Para Ubuntu:

     > **Note**
     >
     > Omite este paso para Ubuntu 22.04.

     ```
     $ tar -xf amdgpu-pro*ubuntu*.xz
     ```

9. Cambie a la carpeta del controlador extraído.
10. Agregue los módulos que faltan para la instalación del controlador.

    - Para Amazon Linux 2 y CentOS:

      Omita este paso.

    - Para Ubuntu:

> **Note**
>
> Omite este paso para Ubuntu 22.04.

```
$ sudo apt install linux-modules-extra-$(uname -r) -y
```

11. Ejecute el script de autoinstalación para instalar la pila de gráficos completa.

    - Para Ubuntu 22.04:

      ```
      $ sudo amdgpu-install --usecase=workstation --vulkan=pro --opencl=rocr,legacy -y
      ```

    - Para Amazon Linux 2 y CentOS y otras versiones de Ubuntu:

      ```
      $ ./amdgpu-pro-install -y --opencl=pal,legacy
      ```

12. Reinicie la instancia.

    ```
    $ sudo reboot
    ```

13. Confirme que el controlador está funcionando.

    ```
    $ dmesg | grep amdgpu
    ```

    La respuesta debe ser similar a la siguiente:

    ```
    Initialized amdgpu
    ```

Instalación del controlador AMD en su instancia de Windows

1. Conéctese a su instancia de Windows y abra una ventana de PowerShell.
2. Configure las credenciales predeterminadas para AWS Tools for Windows PowerShell en su instancia de Windows. Para obtener más información acerca de Cómo empezar a trabajar con AWS Tools for Windows PowerShell consulte la Guía del usuario de AWS Tools for Windows PowerShell.

> **Important**
>
> Su usuario o rol deben tener los permisos concedidos que contiene la política AmazonS3ReadOnlyAccess. Para obtener más información, consulte la política administrada de AWS: AmazonS3ReadOnlyAccess en la Guía del usuario de Amazon Simple Storage Service.

3. Descargue los controladores desde Amazon S3 el escritorio mediante los siguientes comandos de PowerShell.

```
$Bucket = "ec2-amd-windows-drivers"
$KeyPrefix = "latest" # use "archives" for Windows Server 2016
$LocalPath = "$home\Desktop\AMD"
$Objects = Get-S3Object -BucketName $Bucket -KeyPrefix $KeyPrefix -Region us-east-1
foreach ($Object in $Objects) {
$LocalFileName = $Object.Key
if ($LocalFileName -ne '' -and $Object.Size -ne 0) {
    $LocalFilePath = Join-Path $LocalPath $LocalFileName
    Copy-S3Object -BucketName $Bucket -Key $Object.Key -LocalFile $LocalFilePath -
Region us-east-1
}
}
```

4. Descomprima el archivo del controlador descargado y ejecute el instalador con los siguientes comandos de PowerShell.

```
Expand-Archive $LocalFilePath -DestinationPath "$home\Desktop\AMD\$KeyPrefix" -
Verbose
```

Ahora, compruebe el contenido del directorio nuevo. El nombre del directorio se puede recuperar mediante el comando `Get-ChildItem` de PowerShell.

```
Get-ChildItem "$home\Desktop\AMD\$KeyPrefix"
```

El resultado debería ser similar al siguiente:

```
Directory: C:\Users\Administrator\Desktop\AMD\latest

Mode                 LastWriteTime         Length Name
```

```
----                 -------------         ------ ----
d-----       10/13/2021  12:52 AM                210414a-365562C-Retail_End_User.2
```

Instale los controladores de AMD:

```
pnputil /add-driver $home\Desktop\AMD\$KeyPrefix\*.inf /install /subdirs
```

5. Siga las instrucciones para instalar el controlador y reiniciar la instancia como sea necesario.
6. Para verificar que la GPU funciona correctamente, compruebe el administrador de dispositivos. Debería ver «AMD Radeon Pro V520 MxGPU» en la lista como adaptador de pantalla.
7. Para poder aprovechar las cuatro pantallas de resolución de hasta 4K, configure el protocolo de pantalla de alto rendimiento, NICE DCV.

Configuración de un escritorio interactivo para Linux

Después de confirmar que la instancia de Linux tiene instalado el controlador GPU de AMD y amdgpu está en uso, puede instalar un administrador de escritorio interactivo. Recomendamos el entorno de escritorio MATE para obtener la mejor compatibilidad y rendimiento.

Requisito previo

Abra un editor de texto y guarde lo siguiente como archivo denominado `xorg.conf`. Necesitará este archivo en su instancia.

```
Section "ServerLayout"
Identifier     "Layout0"
Screen          0 "Screen0"
InputDevice     "Keyboard0" "CoreKeyboard"
InputDevice     "Mouse0" "CorePointer"
EndSection
Section "Files"
ModulePath "/opt/amdgpu/lib64/xorg/modules/drivers"
ModulePath "/opt/amdgpu/lib/xorg/modules"
ModulePath "/opt/amdgpu-pro/lib/xorg/modules/extensions"
ModulePath "/opt/amdgpu-pro/lib64/xorg/modules/extensions"
ModulePath "/usr/lib64/xorg/modules"
ModulePath "/usr/lib/xorg/modules"
EndSection
Section "InputDevice"
# generated from default
Identifier     "Mouse0"
```

```
Driver         "mouse"
Option         "Protocol" "auto"
Option         "Device" "/dev/psaux"
Option         "Emulate3Buttons" "no"
Option         "ZAxisMapping" "4 5"
EndSection
Section "InputDevice"
# generated from default
Identifier     "Keyboard0"
Driver         "kbd"
EndSection
Section "Monitor"
Identifier     "Monitor0"
VendorName     "Unknown"
ModelName      "Unknown"
EndSection
Section "Device"
Identifier     "Device0"
Driver         "amdgpu"
VendorName     "AMD"
BoardName      "Radeon MxGPU V520"
BusID          "PCI:0:30:0"
EndSection
Section "Extensions"
Option         "DPMS" "Disable"
EndSection
Section "Screen"
Identifier     "Screen0"
Device         "Device0"
Monitor        "Monitor0"
DefaultDepth   24
Option         "AllowEmptyInitialConfiguration" "True"
SubSection "Display"
    Virtual    3840 2160
    Depth      32
EndSubSection
EndSection
```

Para configurar un escritorio interactivo en Amazon Linux 2

1. Instale el repositorio EPEL.

```
$ C:\> sudo amazon-linux-extras install epel -y
```

2. Instale el escritorio MATE.

```
$ C:\> sudo amazon-linux-extras install mate-desktop1.x -y
$ C:\> sudo yum groupinstall "MATE Desktop" -y
$ C:\> sudo systemctl disable firewalld
```

3. Copie el `xorg.conf` archivo en `/etc/X11/xorg.conf`.
4. Reinicie la instancia.

```
$ C:\> sudo reboot
```

5. (Opcional) Instale el servidor NICE DCV para utilizar NICE DCV como protocolo de visualización de alto rendimiento y, a continuación, conéctese a una sesión NICE DCV utilizando su cliente preferido.

Para configurar un escritorio interactivo en Ubuntu

1. Instale el escritorio MATE.

```
$ sudo apt install xorg-dev ubuntu-mate-desktop -y
$ C:\> sudo apt purge ifupdown -y
```

2. Copie el `xorg.conf` archivo en `/etc/X11/xorg.conf`.
3. Reinicie la instancia.

```
$ sudo reboot
```

4. Instale el codificador AMF para la versión de Ubuntu correcta.

```
$ sudo apt install ./amdgpu-pro-20.20-*/amf-amdgpu-pro_20.20-*_amd64.deb
```

5. (Opcional) Instale el servidor NICE DCV para utilizar NICE DCV como protocolo de visualización de alto rendimiento y, a continuación, conéctese a una sesión NICE DCV utilizando su cliente preferido.
6. Después de la instalación de DCV, otorgue permisos de video al usuario de DCV:

```
$ sudo usermod -aG video dcv
```

Para configurar un escritorio interactivo en CentOS

1. Instale el repositorio EPEL.

```
$ sudo yum update -y
$ C:\> sudo yum install epel-release -y
```

2. Instale el escritorio MATE.

```
$ sudo yum groupinstall "MATE Desktop" -y
$ C:\> sudo systemctl disable firewalld
```

3. Copie el `xorg.conf` archivo en `/etc/X11/xorg.conf`.
4. Reinicie la instancia.

```
$ sudo reboot
```

5. (Opcional) Instale el servidor NICE DCV para utilizar NICE DCV como protocolo de visualización de alto rendimiento y, a continuación, conéctese a una sesión NICE DCV utilizando su cliente preferido.

Controladores paravirtuales para instancias de Windows

Las AMI de Windows incluyen un conjunto de controladores para permitir el acceso a hardware virtualizado. Estos controladores los utiliza Amazon EC2 para asignar el almacén de instancias y los volúmenes de Amazon EBS a los dispositivos. En la tabla siguiente se muestran las diferencias principales que existen entre los diferentes controladores.

	RedHat PV	Citrix PV	AWS PV
Tipo de instancia	No compatible con todos los tipos de instancias. Si especific a un tipo de instancia no compatible, la instancia estará dañada.	Compatible con los tipos de instancia Xen.	Compatible con los tipos de instancia Xen.
Volúmenes adjuntos	Admite hasta 16 volúmenes adjuntos.	Admite más de 16 volúmenes adjuntos.	Admite más de 16

	RedHat PV	Citrix PV	AWS PV
			volúmenes adjuntos.
Red	El controlador tiene problemas conocidos de conexión de red que se restablece con cargas elevadas, por ejemplo, con la transferencia rápida de archivos FTP.		El controlador configura automáticamente tramas gigantes en el adaptador de red cuando está en un tipo de instancia compatible. Cuando la instancia está en un grupo con ubicación en clúster, ofrece mejor rendimiento de red entre las instancias que están en el grupo. Para obtener más información, consulte Grupos de ubicación.

En la tabla siguiente se muestran los controladores PV que hay que ejecutar con cada versión de Windows Server en Amazon EC2.

Windows Server versión	Controlador PV versión
Windows Server 2022	Versión más reciente de AWS PV
Windows Server 2019	Versión más reciente de AWS PV
Windows Server 2016	Versión más reciente de AWS PV
Windows Server 2012 R2	Versión más reciente de AWS PV
Windows Server 2012	Versión más reciente de AWS PV
Windows Server 2008 R2	PV de AWS, versión 8.3.5
Windows Server 2008	Citrix PV 5.9
Windows Server 2003	Citrix PV 5.9

Contenido

Controladores AWS PV

Los controladores AWS PV se almacenan en el directorio `%ProgramFiles%\Amazon\Xentools`. Este directorio también contiene símbolos públicos y una herramienta de línea de comandos, `xenstore_client.exe`, que permite el acceso a las entradas de XenStore. Por ejemplo, el siguiente comando de ejemplo PowerShell devuelve la hora actual del Hypervisor:

```
PS C:\> [DateTime]::FromFileTimeUTC((gwmi -n root\wmi -cl
 AWSXenStoreBase).XenTime).ToString("hh:mm:ss")
11:17:00
```

Los componentes del controlador AWS PV se enumeran en el Registro de Windows en `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services`. Estos componentes de controladores son los siguientes: xenbus, xeniface, xennet, xenvbd, y xenvif.

Los controladores AWS PV también tienen un servicio de Windows denominado LiteAgent, que se ejecuta en modo de usuario. Se encarga de tareas como el cierre y el reinicio de los eventos de las API de AWS en instancias de la generación Xen. Puede obtener acceso a los servicios y administrarlos ejecutando `Services.msc` en la línea de comandos. Cuando se ejecutan instancias de la generación Nitro, los controladores AWS PV no se utilizan y el servicio LiteAgent dejará él mismo de iniciarse con la versión del controlador 8.2.4. La actualización al controlador AWS PV más reciente actualiza también el servicio LiteAgent y mejora la fiabilidad de todas las generaciones de instancias.

Instalación de los controladores AWS PV más recientes

Las AMI de Windows para Amazon incluyen un conjunto de controladores que permiten el acceso a hardware virtualizado. Estos controladores los utiliza Amazon EC2 para asignar el almacén de instancias y los volúmenes de Amazon EBS a los dispositivos. Se recomienda instalar los últimos controladores para mejorar la estabilidad y el rendimiento de las instancias de Windows en EC2.

Opciones de instalación

- Para usar AWS Systems Manager para actualizar de manera automática los controladores PV. Para obtener más información, consulte Tutorial: actualización automática de los controladores PV en las instancias de EC2 de Windows (Consola) en la Guía del usuario de AWS Systems Manager.
- Puede descargar el paquete de instalación y ejecutar el programa de instalación manualmente. Asegúrese de comprobar los requisitos del sistema del archivo `readme.txt`. Para obtener más información acerca de la descarga y la instalación de los controladores AWS PV, o la actualización de un controlador de dominio, consulta Actualización manual de las instancias de Windows Server (actualización de controladores de PV de AWS).

Historial de paquetes de controladores AWS PV

En la siguiente tabla se muestran los cambios realizados en cada versión de los controladores AWS PV.

Versión de paquete	Detalles	Fecha de la versión
8.4.3	Se han corregido errores en el instalador del paquete para mejorar la experiencia de actualización.	24 de enero de 2023
8.4.2	Correcciones de estabilidad para solucionar la condición de carrera.	13 de abril de 2022
8.4.1	Instalador de paquetes mejorado.	7 de enero de 2022
8.4.0	• Correcciones de estabilidad para solucionar casos excepcion ales de E/S de disco atascadas. • Correcciones de estabilidad para solucionar casos excepcion ales de bloqueos durante la separación de volumen de EBS. • Función agregada para distribuir la carga entre varios núcleos para cargas de trabajo que aprovechan más de 20 000 IOPS y experimentan degradación debido a cuellos de botella. Para habilitar esta característica, consulte Las cargas de trabajo que aprovechan más de 20 000 IOPS de disco se degradan debido a cuellos de botella de CPU. • La instalación de AWS PV 8.4 en Windows Server 2008 R2 producirá un error. AWS La versión 8.3.5 y las anteriores del PV son compatibles con Windows Server 2008 R2.	2 de marzo de 2021
8.3.5	Instalador de paquetes mejorado.	7 de enero de 2022
8.3.4	Se ha mejorado la fiabilidad del accesorio de dispositivos de red.	4 de agosto de 2020
8.3.3	• Actualice al componente orientado a XenStore-para evitar que se comprueben errores durante las rutas de control de errores. • Actualice al componente de almacenamiento para evitar que se produzcan bloqueos cuando se envíe un SRB no válido.	4 de febrero de 2020

Versión de paquete	Detalles	Fecha de la versión
	Para actualizar este controlador en instancias de Windows Server 2008 R2, primero debe comprobar que se instalen los parches correspondientes a los siguientes avisos de seguridad de Microsoft: Microsoft Security Advisory 3033929.	
8.3.2	Fiabilidad mejorada de los componentes de red.	30 de julio de 2019
8.3.1	Mejoras de rendimiento y robustez en el componente de almacenamiento.	12 de junio de 2019
8.2.7	Eficiencia mejorada para ser compatible con la migración de los tipos de instancias más recientes.	20 de mayo de 2019
8.2.6	Mayor eficacia de la ruta de volcado bloqueado.	15 de enero de 2019
8.2.5	Mejoras de seguridad adicionales. El instalador de PowerShell ya está disponible en el paquete.	12 de diciembre de 2018
8.2.4	Mejoras de fiabilidad.	2 de octubre de 2018
8.2.3	Correcciones de errores y mejoras de rendimiento. Notificar ID de volumen de EBS como número de serie de disco para volúmenes de EBS. Esto habilita situaciones de clúster como S2D.	29 de mayo de 2018
8.2.1	Mejoras de rendimiento de red y almacenamiento además de varias correcciones de solidez. Para verificar que esta versión se ha instalado, consulte el siguiente valor del Registro de Windows: `HKLM\Software\Amazon\PVDriver\Version 8.2.1` .	8 de marzo de 2018

Versión de paquete	Detalles	Fecha de la versión
7.4.6	Correcciones en la estabilidad para que los controladores AWS PV sean más resistentes.	26 de abril de 2017
7.4.3	Compatibilidad añadida para Windows Server 2016. Correcciones en la estabilidad para todas las versiones del sistema operativo Windows compatibles. *La firma del controlador AWS PV versión 7.4.3 caduca el 29 de marzo de 2019. Le recomendamos que actualice al controlador AWS PV más reciente.	18 de noviembre de 2016
7.4.2	Correcciones en la estabilidad para el tipo de instancia X1.	2 de agosto de 2016
7.4.1	• Mejora en el rendimiento del controlador de almacenamiento AWS PV. • Correcciones en la estabilidad del controlador de almacenamiento AWS PV: corrección de un error por el que las instancias llegaban a un bloqueo del sistema con código de comprobación de errores 0x0000DEAD. • Correcciones en la estabilidad del controlador de red AWS PV. • Compatibilidad añadida para Windows Server 2008R2.	12 de julio de 2016
7.3.2	• Registro y diagnóstico mejorados. • Corrección en la estabilidad del controlador de almacenamiento AWS PV. En algunos casos, los discos tal vez no emerjan en Windows después de adjuntarlos de nuevo a la instancia. • Compatibilidad añadida para Windows Server 2012.	24 de junio de 2015

Versión de paquete	Detalles	Fecha de la versión
7.3.1	Actualización de TRIM: corrección relacionada con las solicitudes de TRIM. Esta corrección estabiliza y mejora el rendimiento de las instancias cuando se administra una cantidad grande de solicitudes TRIM.	
7.3.0	Compatibilidad TRIM: ahora el controlador AWS PV envía solicitudes TRIM al hypervisor. Los discos efímeros procesarán correctamente las solicitudes TRIM si el almacenamiento subyacente admite TRIM (SSD). Observe que el almacenamiento con respaldo en EBS no admite TRIM desde marzo de 2015.	
7.2.5	• Corrección en la estabilidad de los controladores de almacenamiento AWS PV: en algunos casos, el controlador AWS PV podía quitar la referencia de memoria no válida y provocar un error del sistema. • Corrección en la estabilidad al generar un volcado de memoria: en algunos casos, el controlador AWS PV podía encontrarse atrapado en una situación de carrera al escribir un volcado de memoria. Antes de la inicialización, este problema solo se resolvía forzando la detención del controlador y reiniciándolo para perder el volcado de memoria.	
7.2.4	Persistencia del ID de dispositivo: esta corrección enmascara el ID de dispositivo de PCI de plataforma y fuerza al sistema a mostrar siempre el mismo ID de dispositivo, aunque la instancia se haya movido. En general, esta corrección afecta al modo en que el hypervisor muestra los dispositivos virtuales. La corrección también incluye modificaciones en el coinstalador de los controladores AWS PV para que el sistema mantenga los dispositivos virtuales asignados.	

Versión de paquete	Detalles	Fecha de la versión
7.2.2	• Carga de los controladores AWS PV en el modo de restauración de servicios de directorio (Directory Services Restore Mode, DSRM): el modo de restauración de servicios de directorio es una opción de arranque en modo seguro de los controladores de dominio de Windows Server. • Mantiene el ID del dispositivo cuando se vuelve a adjuntar el dispositivo adaptador de red virtual: esta corrección fuerza al sistema a comprobar el mapeo de direcciones MAC y mantiene el ID de dispositivo. Esta corrección asegura que los adaptadores retienen la configuración estática si se vuelven a adjuntar.	
7.2.1	• Ejecución en modo seguro: corregido un error que impedía que el controlador cargara en modo seguro. Antes, los controladores AWS PV solo se iniciaban en sistemas de ejecución normal. • Agregar discos a los grupos de almacenamiento de Microsoft Windows: antes sintetizábamos las consultas de página 83. Esta corrección deshabilitó la compatibilidad con página 83. Observe que esto no afecta a los grupos de almacenamiento que se utilizan en un entorno de clúster porque los discos PV no son discos de clúster válidos.	
7.2.0	Base: La versión base de AWS PV.	

Controladores Citrix PV

Los controladores Citrix PV se almacenan en el directorio `%ProgramFiles%\Citrix\XenTools` (instancias de 32 bits) o `%ProgramFiles(x86)%\Citrix\XenTools` (instancias de 64 bits).

Los componentes del controlador Citrix PV se muestran en el Registro de Windows bajo `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services`. Estos componentes son los siguientes: xenevtchn, xeniface, xennet, Xennet6, xensvc, xenvbd y xenvif.

Citrix también tiene un componente de controlador llamado XenGuestAgent, que se ejecuta como un servicio de Windows. Se encarga de tareas como el cierre y reinicio de los eventos de la API. Puede obtener acceso a los servicios y administrarlos ejecutando `Services.msc` en la línea de comandos.

Si se encuentra problemas de redes cuando trabaja con ciertas cargas de trabajo, es posible que tenga que deshabilitar la característica TCP offloading del controlador Citrix PV. Para obtener más información, consulte TCP Offloading.

Controladores RedHat PV

Los controladores RedHat se admiten con las instancias heredadas, pero no se recomiendan con instancias nuevas con más de 12 GB de RAM debido a sus limitaciones. Las instancias con más de 12 GB de RAM que ejecutan controladores RedHat pueden dar error de arranque y quedar inaccesibles. Se recomienda actualizar los controladores RedHat a controladores Citrix PV y, a continuación, actualizar los controladores Citrix PV a controladores AWS PV.

Los archivos de origen de los controladores RedHat se encuentran en el directorio `%ProgramFiles%\RedHat` (instancias de 32 bits) o `%ProgramFiles(x86)%\RedHat` (instancias de 64 bits). Los dos controladores son `rhelnet`, el controlador de red paravirtualizado RedHat y el controlador de minipuerto RedHat SCSI `rhelscsi`.

Suscribirse a las notificaciones de

Amazon SNS puede notificarle cuando se publiquen nuevas versiones de los controladores de Windows para EC2. Para suscribirse a estas notificaciones, utilice uno de los siguientes procedimientos.

> **Note**
>
> Debe especificar la región del tema de SNS al que se suscribe.

Suscripción a las notificaciones de EC2 desde la consola

1. Abra la consola de Amazon SNS en https://console.aws.amazon.com/sns/v3/home.
2. En la barra de navegación, cambie la región a EE. UU. Este (Norte de Virginia), si es necesario. Debe seleccionar esta región porque las notificaciones de SNS a las que se va a suscribir están en esa región.
3. En el panel de navegación, seleccione Subscriptions.

4. Seleccione Create subscription.
5. En el cuadro de diálogo Crear suscripción, haga lo siguiente:
   a. En ARN de tema, copie el siguiente nombre de recurso de Amazon (ARN):

      arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers

   b. En Protocol (Protocolo), elija `Email`.
   c. En Punto de conexión, escriba una dirección de correo electrónico que pueda utilizar para recibir notificaciones.
   d. Seleccione Create subscription.
6. Debe recibir un correo electrónico de confirmación. Abra el mensaje y siga las instrucciones para completar la suscripción.

Suscripción a las notificaciones de EC2 con la AWS CLI

Para suscribirte a las notificaciones de EC2 con AWS CLI, utiliza el siguiente comando.

```
aws sns subscribe --topic-arn arn:aws:sns:us-east-1:801119661308:ec2-
windows-drivers --region us-east-1 --protocol email --notification-
endpoint YourUserName@YourDomainName.ext
```

Suscripción a las notificaciones de EC2 con la AWS Tools for PowerShell

Para suscribirte a las notificaciones de EC2 con Tools for Windows PowerShell, utiliza el siguiente comando.

```
Connect-SNSNotification -TopicArn 'arn:aws:sns:us-east-1:801119661308:ec2-windows-
drivers' -Region us-east-1 -Protocol email -Endpoint 'YourUserName@YourDomainName.ext'
```

Cuando se publican nuevos controladores de Windows para EC2, enviamos notificaciones a los suscriptores. Si ya no desea recibir estas notificaciones, utilice el siguiente procedimiento para cancelar la suscripción.

Anular la suscripción a las notificaciones del controlador de Windows para Amazon EC2

1. Abra la consola de Amazon SNS en https://console.aws.amazon.com/sns/v3/home.
2. En el panel de navegación, seleccione Subscriptions.

3. Seleccione la casilla de verificación de la suscripción y, a continuación, elija Acciones, Eliminar suscripciones. Cuando se le pida confirmación, seleccione Eliminar.

Actualizar controladores PV en instancias de Windows

Te recomendamos instalar los últimos controladores PV para mejorar la estabilidad y el rendimiento de las instancias de Windows EC2. Las instrucciones de esta página te ayudarán a descargar el paquete de controladores y ejecutar el programa de instalación.

Para comprobar qué controlador utiliza su instancia de Windows

Abre Conexiones de red en el panel de control y ve Conexión de área local. Compruebe si el controlador es uno de los siguientes:

- Dispositivo de red AWS PV
- Adaptador Ethernet Citrix PV
- Controladores RedHat PV NIC

También puede comprobar el resultado del comando `pnputil -e`.

Requisitos del sistema

Asegúrese de verificar el archivo `readme.txt` durante la descarga para conocer los requisitos del sistema.

Contenido

- Actualización de las instancias de Windows Server (actualización de PV de AWS) con el Distribuidor
- Actualización manual de las instancias de Windows Server (actualización de controladores de PV de AWS)
- Actualice un controlador de dominio (actualización de AWS PV)
- Actualizar las instancias de Windows Server 2008 y 2008 R2 (actualización de Redhat a Citrix PV)
- Actualizar el servicio Guest Agent de Citrix Xen

Actualización de las instancias de Windows Server (actualización de PV de AWS) con el Distribuidor

Puede usar el Distribuidor, una capacidad de AWS Systems Manager, para instalar o actualizar el paquete de controladores de PV de AWS. La instalación o la actualización se pueden llevar a cabo una sola vez. O bien, puede instalar o actualizar según una programación. La opción `In-place update` de Tipo de instalación no se admite en este paquete del Distribuidor.

> **Important**
>
> Si la instancia es un controlador de dominio, vea Actualice un controlador de dominio (actualización de AWS PV). El proceso de actualización de estas instancias de controlador de dominio es diferente que en las ediciones estándar de Windows.

1. Le recomendamos crear una copia de seguridad en caso de que necesite revertir los cambios.

   > **Tip**
   >
   > En lugar de crear la AMI desde la consola de Amazon EC2, puede utilizar la Automatización de Systems Manager para crear la AMI utilizando el manual de procedimientos de `AWS-CreateImage`. Para obtener más información, consulte AWS-CreateImage en la Guía del usuario de referencia del manual de procedimientos de AWS Systems Manager.

   a. Cuando detiene una instancia, se borran los datos contenidos en todos los volúmenes de almacén de instancias. Antes de detener una instancia, compruebe que ha copiado los datos que necesita de los volúmenes de almacén de instancias al almacenamiento persistente, como Amazon EBS o Amazon S3.
   b. En el panel de navegación, elija Instances (Instancias).
   c. Selecciona la instancia que requiere la actualización del controlador, selecciona Estado de instancia y a continuación selecciona Detener instancia.
   d. Una vez detenida la instancia, selecciona la instancia, selecciona Acciones, luego selecciona Imagen y plantillas y a continuación selecciona Crear imagen.
   e. Elija Instance state (Estado de la instancia) y Start instance (Iniciar instancia).

2. Conéctate a la instancia utilizando una aplicación de escritorio remoto. Para obtener más información, consulte the section called “Conexión a la instancia de Windows mediante un cliente RDP”.
3. Recomendamos que desconecte todos los discos que no sean de sistema y anote los mapeos de letras de unidad a los discos secundarios en Administración de discos antes de realizar esta actualización. Ese paso no es obligatorio si se está llevando a cabo una actualización in situ de los controladores AWS PV. También recomendamos establecer los servicios no esenciales en inicio Manual en la consola de servicios.
4. Para obtener instrucciones sobre cómo instalar o actualizar el paquete de controladores de PV de AWS con el Distribuidor, consulte los procedimientos en Instalación o actualización de paquetes en la Guía del usuario de AWS Systems Manager.
5. En Nombre, elija AWSPVDriver.
6. En Tipo de instalación, seleccione Desinstalar y volver a instalar.
7. Configure los demás parámetros del paquete según sea necesario y ejecute la instalación o la actualización mediante el procedimiento al que se hace referencia en Step 4.

   Después de ejecutar el paquete del Distribuidor, la instancia se reinicia automáticamente y actualiza el controlador. La instancia no estará disponible durante unos 15 minutos como máximo.
8. Una vez completada la actualización y cuando la instancia haya superado las dos comprobaciones de estado en la consola de Amazon EC2, conéctese a la instancia mediante el Escritorio remoto y compruebe que el nuevo controlador se haya instalado.
9. Una vez que se haya conectado, ejecute el siguiente comando de PowerShell:

   ```
   Get-ItemProperty HKLM:\SOFTWARE\Amazon\PVDriver
   ```
10. Verifique que la versión del controlador es la misma versión que la última enumerada en la tabla del historial de versiones del controlador. Para obtener más información, consulte Historial de paquetes de controladores AWS PV. Abra Administración de discos para ver si hay volúmenes secundarios sin conexión y póngalos en línea de modo que se correspondan con las letras de unidad que anotó en Step 3.

Si deshabilitó previamente TCP Offloading mediante Netsh para los controladores Citrix PV, le recomendamos que vuelva a habilitar esta característica después de actualizar a los controladores AWS PV. Los problemas de TCP Offloading con los controladores Citrix no están presentes en

los controladores AWS PV. Como resultado, la TCP Offloading ofrece mejor rendimiento con los controladores AWS PV.

Si anteriormente aplicó una dirección IP estática o una configuración DNS a la interfaz de red, puede tener que volver a aplicar la dirección IP estática o la configuración de DNS después de actualizar los controladores AWS PV.

Actualización manual de las instancias de Windows Server (actualización de controladores de PV de AWS)

Utilice los siguientes procedimientos para llevar a cabo una actualización in situ de los controladores AWS PV o para actualizar los controladores Citrix PV a AWS PV en Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 o Windows Server 2022. Esta actualización no está disponible para los controladores RedHat ni para otras versiones de Windows Server.

Algunas versiones anteriores de Windows Server no pueden usar los controladores más recientes. Para comprobar qué versión de controlador usar en el sistema operativo, consulte la tabla de versiones de controladores en la página Controladores paravirtuales para instancias de Windows.

> **Important**
>
> Si la instancia es un controlador de dominio, vea Actualice un controlador de dominio (actualización de AWS PV). El proceso de actualización de estas instancias de controlador de dominio es diferente que en las ediciones estándar de Windows.

Actualización manual de los controladores de PV de AWS

1. Le recomendamos crear una copia de seguridad en caso de que necesite revertir los cambios.

   > **Tip**
   >
   > En lugar de crear la AMI desde la consola de Amazon EC2, puede utilizar la Automatización de Systems Manager para crear la AMI utilizando el manual de procedimientos de `AWS-CreateImage`. Para obtener más información, consulte AWS-CreateImage en la Guía del usuario de referencia del manual de procedimientos de AWS Systems Manager.

a. Cuando detiene una instancia, se borran los datos contenidos en todos los volúmenes de almacén de instancias. Antes de detener una instancia, compruebe que ha copiado los datos que necesita de los volúmenes de almacén de instancias al almacenamiento persistente, como Amazon EBS o Amazon S3.

b. En el panel de navegación, elija Instances (Instancias).

c. Selecciona la instancia que requiere la actualización del controlador, selecciona Estado de instancia y a continuación selecciona Detener instancia.

d. Una vez detenida la instancia, selecciona la instancia, selecciona Acciones, luego selecciona Imagen y plantillas y a continuación selecciona Crear imagen.

e. Elija Instance state (Estado de la instancia) y Start instance (Iniciar instancia).

2. Conéctate a la instancia utilizando una aplicación de escritorio remoto.

3. Recomendamos que desconecte todos los discos que no sean de sistema y anote los mapeos de letras de unidad a los discos secundarios en Administración de discos antes de realizar esta actualización. Ese paso no es obligatorio si se está llevando a cabo una actualización in situ de los controladores AWS PV. También recomendamos establecer los servicios no esenciales en inicio Manual en la consola de servicios.

4. Descargue el último paquete del controlador en la instancia.

   O ejecute el comando de PowerShell siguiente:

```
Invoke-WebRequest https://s3.amazonaws.com/ec2-windows-drivers-downloads/AWSPV/
Latest/AWSPVDriver.zip -outfile $env:USERPROFILE\pv_driver.zip
Expand-Archive $env:userprofile\pv_driver.zip -DestinationPath
 $env:userprofile\pv_drivers
```

> **Note**
>
> Si recibe un error al descargar el archivo y está usando Windows Server 2016 o una versión anterior, es posible que sea necesario habilitar TLS 1.2 para su terminal PowerShell. Puede habilitar TLS 1.2 para la sesión actual de PowerShell con el siguiente comando y luego volver a intentarlo:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol =
>  [Net.SecurityProtocolType]::Tls12
> ```

5. Extraiga el contenido de la carpeta y después ejecute `AWSPVDriverSetup.msi`.

Después de ejecutar MSI, la instancia vuelve a arrancar automáticamente y actualiza el controlador. La instancia no estará disponible durante unos 15 minutos como máximo. Una vez finalizada la actualización y cuando la instancia pase ambas comprobaciones de estado en la consola de Amazon EC2, puede verificar si se ha instalado el nuevo controlador conectándose a la instancia mediante Escritorio remoto y ejecutando el siguiente comando de PowerShell:

```
Get-ItemProperty HKLM:\SOFTWARE\Amazon\PVDriver
```

Verifique que la versión del controlador es la misma versión que la última enumerada en la tabla del historial de versiones del controlador. Para obtener más información, consulte Historial de paquetes de controladores AWS PV. Abra Administración de discos para ver si hay volúmenes secundarios sin conexión y póngalos en línea de modo que se correspondan con las letras de unidad que anotó en Step 3.

Si deshabilitó previamente TCP Offloading mediante Netsh para los controladores Citrix PV, le recomendamos que vuelva a habilitar esta característica después de actualizar a los controladores AWS PV. Los problemas de TCP Offloading con los controladores Citrix no están presentes en los controladores AWS PV. Como resultado, la TCP Offloading ofrece mejor rendimiento con los controladores AWS PV.

Si anteriormente aplicó una dirección IP estática o una configuración DNS a la interfaz de red, puede tener que volver a aplicar la dirección IP estática o la configuración de DNS después de actualizar los controladores AWS PV.

Actualice un controlador de dominio (actualización de AWS PV)

Utilice el siguiente procedimiento en un controlador de dominio para hacer una actualización in situ de los controladores AWS PV o para actualizar de los controladores Citrix PV a los controladores AWS PV.

Para actualizar un controlador de dominio

1. Te recomendamos crear una copia de seguridad del controlador de dominio, en caso de que necesites revertir los cambios. No se admite el uso de una AMI como copia de seguridad. Para obtener más información, consulte Consideraciones de copia de seguridad y restauración para controladores de dominio virtualizados en la documentación de Microsoft.

2. Ejecuta el siguiente comando para configurar Windows de modo que arranque en el modo de restauración de servicios de directorio (DSRM):

> **Warning**
>
> Antes de ejecutar este comando, confirme que sabe la contraseña de DSRM. Necesita ese dato para iniciar sesión en la instancia una vez que termine la actualización y la instancia se reinicie de forma automática.

```
bcdedit /set {default} safeboot dsrepair
```

PowerShell:

```
PS C:\> bcdedit /set "{default}" safeboot dsrepair
```

El sistema debe arrancar en DSRM porque la utilidad de actualización elimina los controladores de almacenamiento Citrix PV para poder instalar los controladores AWS PV. Por lo tanto, recomendamos que anote cualquier mapeo de carpetas y letras de unidad a los discos secundarios en Administración de discos. Cuando los controladores de almacenamiento Citrix PV no están presentes, no se detectarán los controladores secundarios. Los controladores de dominio que usan una carpeta NTDS en los controladores secundarios no arrancarán porque el disco secundario no será detectado.

> **Warning**
>
> Después de ejecutar este comando no arranque de nuevo el sistema manualmente. El sistema no estará alcanzable porque los controladores Citrix PV no admiten DSRM.

3. Ejecute el siguiente comando para añadir **`DisableDCCheck`** al registro:

```
reg add HKLM\SOFTWARE\Wow6432Node\Amazon\AWSPVDriverSetup /v DisableDCCheck /t
 REG_SZ /d true
```

4. Descargue el último paquete del controlador en la instancia.
5. Extraiga el contenido de la carpeta y después ejecute `AWSPVDriverSetup.msi`.

Después de ejecutar MSI, la instancia vuelve a arrancar automáticamente y actualiza el controlador. La instancia no estará disponible durante unos 15 minutos como máximo.

6. Una vez finalizada la actualización y de que la instancia pase ambas comprobaciones de estado en la consola de Amazon EC2, conéctese a la instancia mediante el Escritorio remoto. Abre Administración de discos para ver si hay volúmenes secundarios fuera de línea y ponlos en línea de modo que se correspondan con las letras de controlador y las asignaciones de carpetas que anotaste previamente.

   Debe conectarse a la instancia especificando el nombre de usuario con el formato siguiente hostname\administrator. Por ejemplo, Win2k12TestBox\administrator.

7. Ejecute el siguiente comando para quitar la configuración de arranque de DSRM:

   ```
   bcdedit /deletevalue safeboot
   ```

8. Reinicie la instancia.

9. Para completar el proceso de actualización, verifique que se ha instalado el nuevo controlador. En Administrador de dispositivos, en Controladores de almacenamiento, localice Adaptador de host de almacenamiento PV de AWS. Verifique que la versión del controlador es la misma versión que la última enumerada en la tabla del historial de versiones del controlador. Para obtener más información, consulte Historial de paquetes de controladores AWS PV.

10. Ejecute el siguiente comando para eliminar **`DisableDCCheck`** del registro:

    ```
    reg delete HKLM\SOFTWARE\Wow6432Node\Amazon\AWSPVDriverSetup /v DisableDCCheck
    ```

> **Note**
>
> Si deshabilitó previamente TCP Offloading mediante Netsh para los controladores Citrix PV, le recomendamos que vuelva a habilitar esta característica después de actualizar a los controladores AWS PV. Los problemas de TCP Offloading con los controladores Citrix no están presentes en los controladores AWS PV. Como resultado, la TCP Offloading ofrece mejor rendimiento con los controladores AWS PV.

Actualizar las instancias de Windows Server 2008 y 2008 R2 (actualización de Redhat a Citrix PV)

Antes de comenzar la actualización de los controladores RedHat a controladores Citrix PV, asegúrese de hacer lo siguiente:

- Instalar la última versión del servicio EC2Config. Para obtener más información, consulte Instalar la versión más reciente de EC2Config.
- Verifique si tiene Windows PowerShell 3.0 instalado. Para verificar la versión que ha instalado, ejecute el comando siguiente en la ventana de PowerShell:

  ```
  PS C:\> $PSVersionTable.PSVersion
  ```

  Windows PowerShell 3.0 se incluye en el paquete de instalación de la versión 3.0 Windows Management Framework (WMF). Si necesita instalar Windows PowerShell 3.0, consulte Windows Management Framework 3.0 en el Centro de descarga de Microsoft.
- Haga copia de back up de la información importante de la instancia o cree una AMI desde la instancia. Para obtener más información sobre cómo crear una AMI, consulte Creación de una AMI basada en Amazon EBS.

  > **Tip**
  >
  > En lugar de crear la AMI desde la consola de Amazon EC2, puede utilizar la Automatización de Systems Manager para crear la AMI utilizando el manual de procedimientos de `AWS-CreateImage`. Para obtener más información, consulte AWS-CreateImage en la Guía del usuario de referencia del manual de procedimientos de AWS Systems Manager.

  Si crea una AMI, asegúrese de hacer lo siguiente:

  - Apunte la contraseña.
  - No ejecute la herramienta Sysprep manualmente ni use el servicio EC2Config.
  - Establezca el adaptador Ethernet para que obtenga una dirección IP automáticamente usando DHCP. Para obtener más información, consulte Configure TCP/IP Settings en Microsoft TechNet Library.

Para actualizar los controladores RedHat

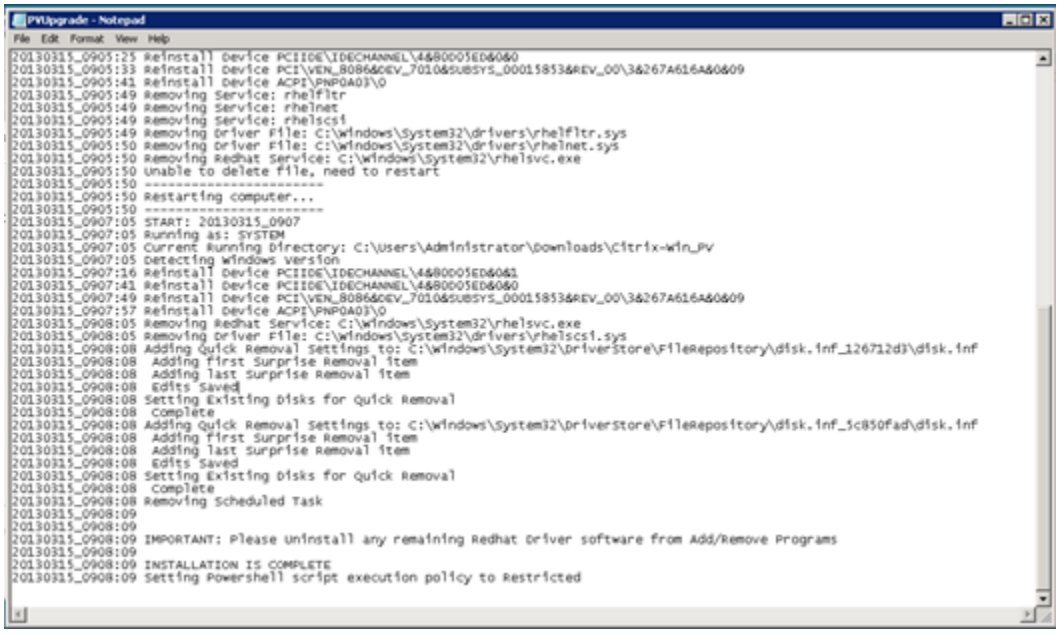
1. Conéctese a la instancia e inicie sesión como administrador local. Para obtener más información sobre cómo conectarse a la instancia, consulte Conexión con la instancia de Windows de.
2. En la instancia, descargue el paquete de actualización de Citrix PV.
3. Extraiga el contenido del paquete de actualización en una ubicación de su elección.
4. Haga doble clic en el archivo Upgrade.bat. Si recibe una advertencia de seguridad, elija Run (Ejecutar).
5. En el cuadro de diálogo Upgrade Drivers (Actualizar controladores), revise la información y elija Yes (Sí) si está preparado para comenzar la actualización.
6. En el cuadro de diálogo Red Hat Paravirtualized Xen Drivers for Windows uninstaller (Desinstalador de Controladores Xen de Red Hat Paravirtualized para Windows), elija Yes (Sí) para eliminar el software de RedHat. La instancia volverá a arrancarse.

> **Note**
>
> Si no ve el cuadro de diálogo del desinstalador, elija Red Hat Paravirtualized en la barra de tareas de Windows.

7. Compruebe que la instancia ha vuelto a arrancar y que está lista para su uso.
   a. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
   b. En la página instancias, selecciona Acciones, luego selecciona Supervisar y solucionar problemasy a continuación selecciona Obtener registro del sistema.
   c. Las operaciones de actualización deberían haber reiniciado el servidor unas tres o cuatro veces. Puede verlo en el archivo de registro según el número de veces que se muestra `Windows is Ready to use`.

```
    Microsoft Windows NT 6.0.6002 Service Pack 2 (en-US)
 Ec2Config service v2.1.9.0
  RedHat PV NIC Driver v1.3.10.0
2013/03/15 17:11:01Z: Waiting for meta-data accessibility...
2013/03/15 17:11:02Z: Meta-data is now available.
<RDPCERTIFICATE>
<THUMBPRINT>D6BFD64F21359516C781CA7DF2821C5EFC35648A</THUMBPRINT>
</RDPCERTIFICATE>
<Username>Administrator</Username>
<Password>
L79ThJPF8LyIL38IZht0FBrjet3vnT2csTiU/XGVMRCH7kQtBnznAnXrKd1sirXlxl9BwVMsd9b38jFJqv0lIUpgNNJRZoCDc7IbUw
</Password>
2013/03/15 17:11:30Z: Product activation was successful.
2013/03/15 17:11:32Z: Message: Windows is Ready to use
Microsoft Windows NT 6.0.6002 Service Pack 2 (en-US)
 Ec2Config service v2.1.9.0
2013/03/15 21:04:24Z: There was an exception writing driver information to console: System.Exception:
   at Ec2Config.Service1.Go()
2013/03/15 21:04:35Z: Waiting for meta-data accessibility...
2013/03/15 21:04:40Z: Meta-data is now available.
<RDPCERTIFICATE>
<THUMBPRINT>D6BFD64F21359516C781CA7DF2821C5EFC35648A</THUMBPRINT>
</RDPCERTIFICATE>
2013/03/15 21:05:08Z: Product activation was successful.
2013/03/15 21:05:09Z: Message: Windows is Ready to use
Microsoft Windows NT 6.0.6002 Service Pack 2 (en-US)
 Ec2Config service v2.1.9.0
  Citrix PV Ethernet Adapter v5.9.960.49119
2013/03/15 21:07:20Z: Waiting for meta-data accessibility...
2013/03/15 21:07:21Z: Meta-data is now available.
<RDPCERTIFICATE>
<THUMBPRINT>D6BFD64F21359516C781CA7DF2821C5EFC35648A</THUMBPRINT>
</RDPCERTIFICATE>
2013/03/15 21:07:27Z: Message: Windows is Ready to use
```

8. Conéctese a la instancia e inicie sesión como administrador local.
9. Cierre el cuadro de diálogo Red Hat Paravirtualized Xen Drivers for Windows uninstaller (Desinstalador de Controladores Xen de Red Hat Paravirtualized para Windows).
10. Confirme que la instalación ha finalizado. Desplácese a la carpeta `Citrix-WIN_PV` que ha descomprimido antes, abra el archivo `PVUpgrade.log` y, después, busque el texto `INSTALLATION IS COMPLETE`.



Actualizar el servicio Guest Agent de Citrix Xen

Si utiliza controladores PV Citrix en Windows Server, puede actualizar el servicio Citrix Xen Guest Agent. Este servicio de Windows se encarga de tareas como el apagado y el reinicio desde la API. Puede ejecutar este paquete de actualización en cualquier versión de Windows Server, siempre que la instancia ejecute controladores PV Citrix.

> **Important**
>
> Para Windows Server 2008 R2 y versiones posteriores, recomendamos que actualice a los controladores AWS PV que incluyen la actualización Guest Agent.

Antes de comenzar la actualización de los controladores, cree una copia de back up de la información importante de la instancia, o bien, cree una AMI a partir de la instancia. Para obtener más información sobre cómo crear una AMI, consulte Creación de una AMI basada en Amazon EBS.

> **Tip**
>
> En lugar de crear la AMI desde la consola de Amazon EC2, puede utilizar la Automatización de Systems Manager para crear la AMI utilizando el manual de procedimientos de `AWS-CreateImage`. Para obtener más información, consulte AWS-CreateImage en la Guía del usuario de referencia del manual de procedimientos de AWS Systems Manager.

Si crea una AMI, asegúrese de que hace lo siguiente:

- No habilite la herramienta Sysprep en el servicio EC2Config.
- Apunte la contraseña.
- Establezca el adaptador Ethernet en DHCP.

Para actualizar el servicio Citrix Xen Guest Agent

1. Conéctese a la instancia e inicie sesión como administrador local. Para obtener más información sobre cómo conectarse a la instancia, consulte Conexión con la instancia de Windows de.
2. En la instancia, descargue el paquete de actualización de Citrix.
3. Extraiga el contenido del paquete de actualización en una ubicación de su elección.

4. Haga doble clic en el archivo Upgrade.bat. Si recibe una advertencia de seguridad, elija Run (Ejecutar).
5. En el cuadro de diálogo Upgrade Drivers (Actualizar controladores), revise la información y elija Yes (Sí) si está preparado para comenzar la actualización.
6. Cuando la actualización finalice, se abrirá el archivo `PVUpgrade.log` con el texto `UPGRADE IS COMPLETE`.
7. Reinicie su instancia.

Cómo solucionar problemas de controladores PV en instancias de Windows

A continuación, se describen las soluciones a los problemas que puedan surgir con las imágenes de Amazon EC2 y los controladores de PV anteriores.

Contenido

Windows Server 2012 R2 pierde la conexión de red y almacenamiento después de volver a arrancar la instancia

> **Important**
>
> Este problema solo se produce con las AMI disponibles antes de septiembre de 2014.

Las imágenes de máquina de Amazon (AMI) para Windows Server 2012 R2 que se pusieron a disposición de los usuarios antes del 10 de septiembre de 2014 pueden perder la conexión de red y de almacenamiento tras reiniciar la instancia. El error del registro del sistema de la AWS Management Console indica: “Difficulty detecting PV driver details for Console Output”. La pérdida de conexión se debe a la característica Plug and Play Cleanup. Esta característica busca y deshabilita los dispositivos inactivos del sistema cada 30 días. La característica identifica incorrectamente el

dispositivo de red de EC2 en estado inactivo y lo elimina del sistema. Cuando ocurre, la instancia pierde la conexión de red después de arranque.

En los sistemas que sospeche que pueden verse afectados por este problema, puede descargar y ejecutar una actualización in situ del controlador. Si no consigue llevar a cabo la actualización in situ, puede ejecutar un script ayudante. El script determina si la instancia está afectada. Si lo está, y el dispositivo de red de Amazon EC2 no se ha eliminado, el script deshabilita el análisis de Plug and Play Cleanup. Si el dispositivo de red se ha eliminado, el script repara el dispositivo, deshabilita el análisis de Plug and Play Cleanup y permite que la instancia arranque con la conexión de red habilitada.

Contenido

Elegir cómo solucionar problemas

Existen dos métodos para restaurar la conexión de red y almacenamiento en una instancia que se ha visto afectada por este problema. Elija uno de los siguientes métodos:

Método	Requisitos previos	Información general del procedimiento
Método 1: Redes mejoradas	Las redes mejoradas solo están disponibles en una nube privada virtual (VPC) que requiere un tipo de instancia C3. Si el servidor no utiliza el tipo de instancia C3, debe cambiarla temporalmente.	Puede cambiar el tipo de instancia de servidor a C3. Las redes mejoradas le permiten conectarse a la instancia afectada y corregir el problema. Después de corregir el problema, cambie la instancia al tipo de instancia original de nuevo. Este método es generalmente más rápido que el método 2 y es menos probable que dé un

Método	Requisitos previos	Información general del procedimiento
		error del usuario. Incurrirá en gastos adicionales mientras que ejecute la instancia C3.
Método 2: Configuración del Registro	Capacidad para crear u obtener acceso a un servidor secundario. Capacidad para cambiar la configuración del Registro.	Separe el volumen raíz de la instancia afectada, adjúntelo a una instancia diferente, conéctese y haga los cambios en el Registro. Incurrirá en gastos adicionales mientras que ejecute el servidor adicional. Este método es más lento que el 1, pero ha dado resultado en situaciones en las que el método 1 no sirvió para resolver el problema.

Método 1: Redes mejoradas

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancias).
3. Localice la instancia afectada. Selecciona la instancia, selecciona Estado de instanciay a continuación selecciona Detener instancia.

   > **Warning**
   >
   > Cuando detiene una instancia, se borran los datos contenidos en todos los volúmenes de almacén de instancias. Para conservar los datos de los volúmenes del almacén de instancias, asegúrese de realizar una copia de seguridad de ellos en un almacenamiento persistente.

4. Una vez que la instancia se haya detenido, cree una copia de seguridad. Selecciona la instancia, selecciona Acciones, luego selecciona Imagen y plantillas y a continuación selecciona Crear imagen.

5. Cambie el tipo de instancia por un tipo de instancia C3.
6. Inicie la instancia.
7. Conéctese a la instancia mediante el Escritorio remoto y descargue el paquete de actualización de los controladores AWS PV en la instancia.
8. Extraiga el contenido de la carpeta y ejecute `AWSPVDriverSetup.msi`.

   Después de ejecutar MSI, la instancia vuelve a arrancar automáticamente y actualiza los controladores. La instancia no estará disponible durante unos 15 minutos como máximo.
9. Una vez finalizada la actualización y de que la instancia pase ambas comprobaciones de estado en la consola de Amazon EC2, conéctese a la instancia mediante el Escritorio remoto y compruebe que los nuevos controladores se han instalado. En Device Manager (Administrador de dispositivos), en Storage Controllers (Controladores de almacenamiento), localice PV Storage Host Adapter (Adaptador de host de almacenamiento de AWS). Verifique que la versión del controlador es la misma versión que la última enumerada en la tabla del historial de versiones del controlador. Para obtener más información, consulte Historial de paquetes de controladores AWS PV.
10. Detenga la instancia y devuélvala a su tipo de instancia original.
11. Inicie la instancia y continúe con el uso normal.

Método 2: Configuración del Registro

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancias).
3. Localice la instancia afectada. Selecciona la instancia, selecciona Estado de instancia y a continuación selecciona Detener instancia.

   > **Warning**
   >
   > Cuando detiene una instancia, se borran los datos contenidos en todos los volúmenes de almacén de instancias. Para conservar los datos de los volúmenes del almacén de instancias, asegúrese de realizar una copia de seguridad de ellos en un almacenamiento persistente.
4. Selecciona iniciar instancias y crea una instancia temporal de Windows Server 2008 o Windows Server 2012 en la misma zona de disponibilidad que la instancia afectada. No cree una instancia de Windows Server 2012 R2.

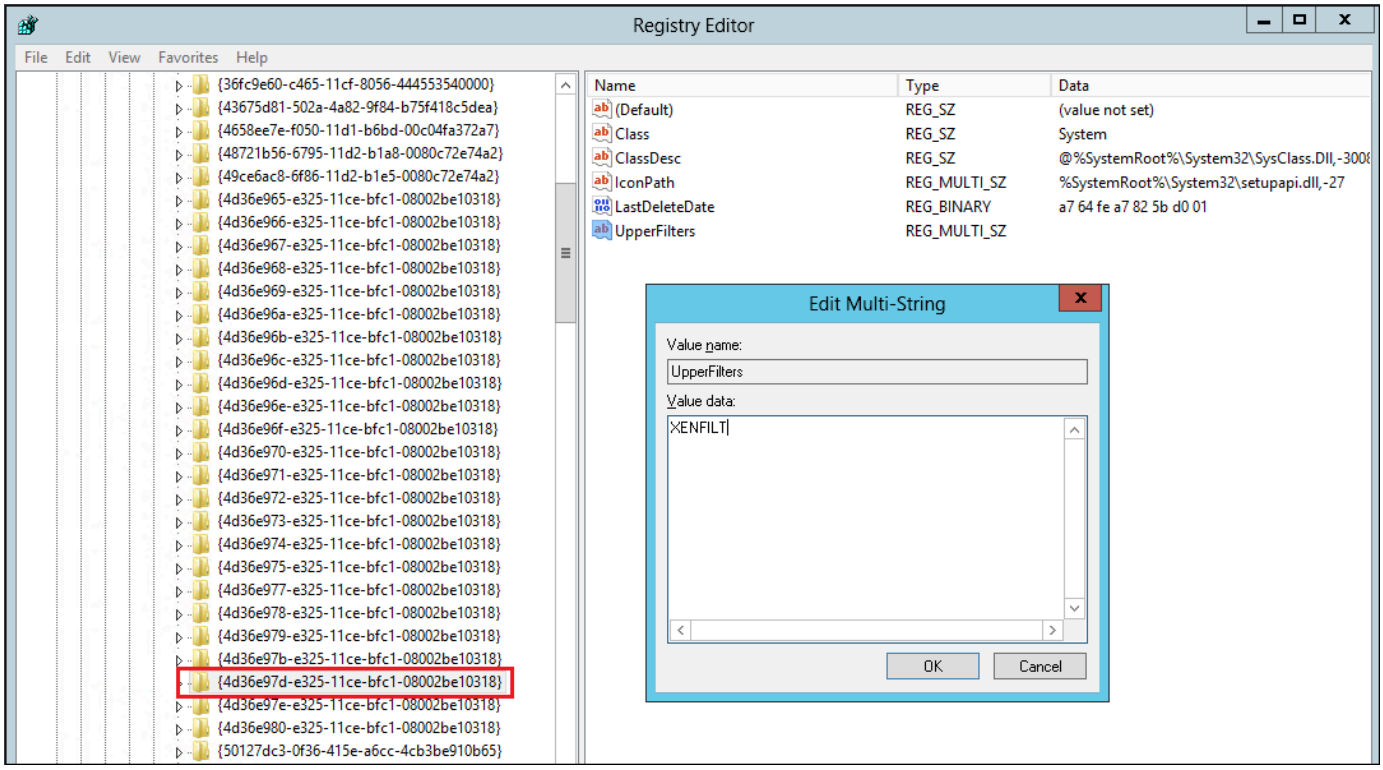
> **Important**
>
> Si no crea la instancia en la misma zona de disponibilidad que la instancia afectada, no podrá adjuntar el volumen raíz de la instancia afectada a la nueva instancia.

5. En el panel de navegación, elija Volumes (Volúmenes).
6. Localice el volumen raíz de la instancia afectada. Desasocie el volumen y asócielo a la instancia temporal que ha creado antes. Adjúntelo con el nombre de dispositivo predeterminado (xvdf).
7. Utilice el Escritorio remoto para conectarse a la instancia temporal y, a continuación, utilice la utilidad de Administración de discos para hacer que el volumen esté disponible para su uso.
8. En la instancia temporal, abra el cuadro de diálogo Ejecutar, escriba **`regedit`** y pulse Intro.
9. En el panel de navegación de Registry Editor (Editor del registro), elija HKEY_LOCAL_MACHINE y en el menú File (Archivo), elija Load Hive (Cargar Hive).
10. En el cuadro de diálogo Load Hive (Cargar Hive), desplácese a Affected Volume (Volumen afectado) \Windows\System32\config\System y escriba un nombre temporal en el cuadro de diálogo Key Name (Nombre de clave). Por ejemplo, escriba OldSys.
11. En el panel de navegación del Editor del Registro, localice las claves siguientes:

    HKEY_LOCAL_MACHINE***`su_nombre_de_clave_temporal`**\ControlSet001\Control\Class\4d36e97d-e325-11ce-bfc1-08002be10318

    HKEY_LOCAL_MACHINE***`su_nombre_de_clave_temporal`**\ControlSet001\Control\Class\4d36e96a-e325-11ce-bfc1-08002be10318

12. Para cada clave, haga doble clic en UpperFilters, escriba un valor para XENFILT y elija Aceptar.



13. Localice la siguiente clave:

    HKEY_LOCAL_MACHINE***su_nombre_de_clave_temporal***\ControlSet001\Services\XENBUS\Parameters

14. Cree una nueva cadena (REG_SZ) con el nombre ActiveDevice y el valor siguiente:

    PCI\VEN_5853&DEV_0001&SUBSYS_00015853&REV_01

15. Localice la siguiente clave:

    HKEY_LOCAL_MACHINE***su_nombre_de_clave_temporal***\ControlSet001\Services\XENBUS

16. Cambie Count de 0 a 1.

17. Localice y elimine las siguientes claves:

    HKEY_LOCAL_MACHINE***su_nombre_de_clave_temporal***\ControlSet001\Services\xenvbd\StartOverride

    HKEY_LOCAL_MACHINE ***su_nombre_de_clave_temporal***\ControlSet001\Services\xenfilt\StartOverride

18. En el panel de navegación del Editor del Registro, elija la clave temporal que creó cuando abrió el Editor del Registro por primera vez.

19. En el menú Archivo, elija Descargar Hive.
20. En la utilidad de Administración de discos, elija la unidad que adjuntó anteriormente, abra el menú contextual (clic con el botón derecho) y elija Sin conexión.
21. En la consola de Amazon EC2, separe el volumen afectado de la instancia temporal y vuelva a adjuntarlo a la instancia de Windows Server 2012 R2 con el nombre de dispositivo /dev/sda1. Debe especificar este nombre de dispositivo para designar el volumen como volumen raíz.
22. Inicie la instancia.
23. Conéctese a la instancia mediante el Escritorio remoto y descargue el paquete de actualización de los controladores AWS PV en la instancia.
24. Extraiga el contenido de la carpeta y ejecute `AWSPVDriverSetup.msi`.

    Después de ejecutar MSI, la instancia vuelve a arrancar automáticamente y actualiza los controladores. La instancia no estará disponible durante unos 15 minutos como máximo.
25. Una vez finalizada la actualización y de que la instancia pase ambas comprobaciones de estado en la consola de Amazon EC2, conéctese a la instancia mediante el Escritorio remoto y compruebe que los nuevos controladores se han instalado. En Device Manager (Administrador de dispositivos), en Storage Controllers (Controladores de almacenamiento), localice PV Storage Host Adapter (Adaptador de host de almacenamiento de AWS). Verifique que la versión del controlador es la misma versión que la última enumerada en la tabla del historial de versiones del controlador. Para obtener más información, consulte Historial de paquetes de controladores AWS PV.
26. Elimine o detenga la instancia temporal que creó en este procedimiento.

Ejecutar el script de corrección activa de errores

Si no consigue llevar a cabo la actualización in situ del controlador ni migrar a una nueva instancia, puede ejecutar el script de corrección para corregir los problemas que ha causado la tarea de Plug and Play Cleanup.

Para ejecutar el script de corrección activa de errores

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancias).
3. Selecciona el nombre de la instancia para la que quieres ejecutar el script de corrección activa de errores. Selecciona Estado de instancia y a continuación selecciona Detener instancia.

> **Warning**
>
> Cuando detiene una instancia, se borran los datos contenidos en todos los volúmenes de almacén de instancias. Para conservar los datos de los volúmenes del almacén de instancias, asegúrese de realizar una copia de seguridad de ellos en un almacenamiento persistente.

4. Una vez que la instancia se haya detenido, cree una copia de seguridad. Selecciona la instancia, selecciona Acciones, luego selecciona Imagen y plantillas y a continuación selecciona Crear imagen.
5. Selecciona Estado de instancia y a continuación selecciona Iniciar instancia.
6. Conéctese a la instancia mediante el Escritorio remoto y descargue la carpeta RemediateDriverIssue.zip en la instancia.
7. Extraiga el contenido de la carpeta.
8. Ejecute el script según las instrucciones del archivo Readme.txt. El archivo se encuentra en el carpeta en la que ha descomprimido RemediateDriverIssue.zip.

TCP Offloading

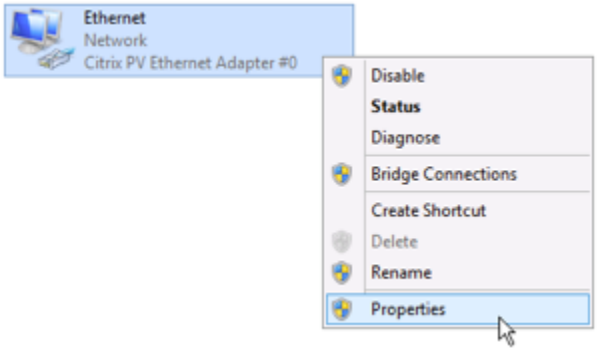
> **Important**
>
> Este problema no se aplica a las instancias que ejecutan los controladores de red AWS PV o Intel.

De manera predeterminada, TCP offloading está habilitado para los controladores Citrix PV en las AMI de Windows. Si encuentra algún error en el transporte o la transmisión de paquetes (visibles en el Monitor de rendimiento de Windows) —por ejemplo, cuando ejecuta determinadas cargas de SQL —, tal vez necesite deshabilitar esta característica.

> **Warning**
>
> Deshabilitar TCP offloading puede reducir el rendimiento de red de la instancia.

Para deshabilitar TCP offloading para Windows Server 2012 y 2008

1. Conéctese a la instancia e inicie sesión como administrador local.
2. Si utiliza Windows Server 2012, presione Ctrl+Esc para obtener acceso a la pantalla Inicio y, a continuación, elija Panel de control. Si utiliza Windows Server 2008, elija Inicio y seleccione Panel de control.
3. Elija Red e Internet y, a continuación, Centro de redes y recursos compartidos.
4. Elija Cambiar configuración del adaptador.
5. Haga clic con el botón derecho en Citrix PV Ethernet Adapter #0 y seleccione Propiedades.



6. En el cuadro de diálogo Propiedades de conexión de área local, elija Configurar para abrir el cuadro de diálogo Propiedades de Citrix PV Ethernet Adapter #0.
7. En la pestaña Opciones avanzadas, deshabilite todas las propiedades excepto Corregir valor de suma de comprobación de TCP/UDP. Para deshabilitar una propiedad, selecciónela en Propiedad y elija Desactivado en Valor.
8. Seleccione OK.
9. En la ventana del símbolo del sistema, ejecute el siguiente comando.

```
netsh int ip set global taskoffload=disabled
netsh int tcp set global chimney=disabled
netsh int tcp set global rss=disabled
netsh int tcp set global netdma=disabled
```

10. Reinicie la instancia.

Sincronización horaria

Antes de la versión 2013.02.13 Windows AMI, Citrix Xen Guest Agent podía establecer la hora del sistema incorrectamente. Esto puede hacer que caduque la concesión de DHCP. Si tiene problemas de conexión con la instancia, es posible que tenga que actualizar el agente.

Para determinar si tiene Citrix Xen guest agent actualizado, compruebe si el archivo `C:\Program Files\Citrix\XenGuestAgent.exe` es de marzo de 2013. Si la fecha de este archivo es anterior, actualice el servicio Citrix Xen Guest Agent. Para obtener más información, consulte Actualizar el servicio Guest Agent de Citrix Xen.

Las cargas de trabajo que aprovechan más de 20 000 IOPS de disco se degradan debido a cuellos de botella de CPU

Puede verse afectado por este problema si utiliza instancias de Windows que ejecutan controladores PV de AWS que aprovechan más de 20 000 IOPS y se presenta un código de comprobación de errores `0x9E: USER_MODE_HEALTH_MONITOR`.

Las lecturas y las escrituras de disco (E/S) en los controladores de AWS PV se realizan en dos fases: Preparación de E/S y Finalización de E/S. De forma predeterminada, la fase de preparación se ejecuta en un único core arbitrario. La fase de finalización se ejecuta en el core `0`. La cantidad de cálculo necesaria para procesar una E/S varía según su tamaño y otras propiedades. Algunas E/S usan más cálculo en la fase de preparación y otros en la fase de finalización. Cuando una instancia impulsa más de 20 000 IOPS, la fase de preparación o finalización puede dar lugar a un cuello de botella, en el que la CPU en la que se ejecuta tiene una capacidad del 100 %. El hecho de que la fase de preparación o finalización se convierta o no en un cuello de botella depende de las propiedades de las E/S utilizada por la aplicación.

A partir de los controladores AWS PV 8.4.0, la carga de la fase de preparación y la fase de finalización se pueden distribuir entre varios núcleos, lo que elimina los cuellos de botella. Cada aplicación utiliza diferentes propiedades de E/S. Por lo tanto, la aplicación de una de las siguientes configuraciones puede aumentar, disminuir o no afectar el rendimiento de la aplicación. Después de aplicar cualquiera de estas configuraciones, monitoree la aplicación para comprobar que cumple con el rendimiento que usted desea.

1. Requisitos previos

   Antes de comenzar este procedimiento de solución de problemas, compruebe los siguientes requisitos previos:

   - La instancia utiliza controladores AWS PV versión 8.4.0 o posteriores. Para actualizar, consulte Actualizar controladores PV en instancias de Windows.
   - Tiene acceso de RDP a la instancia. Para obtener información sobre los pasos para conectarse a la instancia de Windows mediante RDP, consulte Conexión a la instancia de Windows mediante un cliente RDP.

- Tiene acceso de administrador en la instancia.

2. Observar la carga de CPU en la instancia

   Puede usar el Administrador de tareas de Windows para ver la carga en cada CPU y determinar posibles cuellos de botella en E/S del disco.

   1. Compruebe que la aplicación se está ejecutando y maneja tráfico similar a la carga de trabajo de producción.
   2. Conectarse a la instancia mediante RDP
   3. Elija el menú Start (Iniciar) en la instancia.
   4. Introduzca `Task Manager` en el menú Start (Iniciar) para abrir el Administrador de tareas.
   5. Si el Administrador de tareas muestra la vista de resumen, elija More details (Más detalles) para expandir la vista detallada.
   6. Seleccione la pestaña Performance (Desempeño).
   7. Seleccione CPU en el panel izquierdo.
   8. Haga clic con el botón derecho en el gráfico del panel principal y seleccione Change graph to (Cambiar gráfico a)>Logical processors (Procesadores lógicos) para mostrar cada core individual.
   9. Dependiendo de cuántos cores haya en la instancia, puede ver líneas que muestran la carga de CPU a lo largo del tiempo o que simplemente vea un número.
      - Si ve gráficos que muestran la carga a lo largo del tiempo, busque CPU donde la caja esté casi completamente sombreada.
      - Si ve un número en cada core, busque cores que muestren constantemente un 95 % o más.
   10. Tenga en cuenta si el core `0` o un core diferente presentan una carga pesada.

3. Elegir la configuración a aplicar

Nombre de la configuración	Cuándo aplicar esta configuración	Notas
Default configuration	La carga de trabajo está impulsando menos de 20 000 IOPS, u otras configuraciones no	Para esta configuración, la E/S se produce en algunos cores, lo que puede beneficiar cargas de trabajo

Nombre de la configuración	Cuándo aplicar esta configuración	Notas
	mejoraron el rendimiento ni la estabilidad.	más pequeñas al aumentar la ubicación de la caché y reducir la conmutación de contexto.
Allow driver to choose whether to distribute completion	La carga de trabajo impulsa más de 20 000 IOPS y se observa una carga moderada o alta en el core `0`.	Esta configuración se recomienda para todas las instancias de Xen que utilicen PV 8.4.0 o posterior y aprovechen más de 20 000 IOPS, independi entemente de que se detecten problemas o no.
Distribute both preparation and completion	La carga de trabajo está impulsando más de 20 000 IOPS, y permitir que el controlador elija la distribución no mejoró el rendimiento o un core distinto de `0` presenta una carga alta.	Esta configuración permite distribuir tanto la preparación de E/S como su finalización.

> **Note**
>
> Recomendamos que no distribuya la preparación de E/S sin distribuir también la finalización de E/S (configuración `DpcRedirection` sin configuración `NotifierDistributed`) porque la fase de finalización es sensible a la sobrecarga por parte de la fase de preparación cuando la fase de preparación se está ejecutando en paralelo.

Valores de clave del registro

- NotifierDistributed

  Valor `0` o no presente —. La fase de finalización se ejecutará en `0`.

  Valor 1 —. El controlador elige ejecutar la fase de finalización o el core `0` o un core adicional por disco conectado.

  Valor 2 —. El controlador ejecuta la fase de finalización en un core adicional por disco conectado.

- DpcRedirection

  Valor `0` o no presente —. La fase de preparación se ejecutará en un único core arbitrario.

  Valor 1 —. La fase de preparación se distribuye entre varios cores.

Configuración predeterminada

Aplique la configuración predeterminada con las versiones del controlador AWS PV anteriores a la versión 8.4.0, o si se observa una degradación del rendimiento o de la estabilidad después de aplicar una de las otras configuraciones que se detallan en esta sección.

1. Conectarse a la instancia mediante RDP
2. Abra un nuevo símbolo del sistema de PowerShell como administrador.
3. Ejecute los siguientes comandos para quitar las claves de registro `NotifierDistributed` y `DpcRedirection`.

   ```
   Remove-ItemProperty -Path HKLM:\System\CurrentControlSet\Services\xenvbd
   \Parameters -Name NotifierDistributed
   ```

   ```
   Remove-ItemProperty -Path HKLM:\System\CurrentControlSet\Services\xenvbd
   \Parameters -Name DpcRedirection
   ```

4. Reinicie su instancia.

Permitir al controlador elegir si desea distribuir la finalización

Establezca la clave de registro `NotiferDistributed` para permitir que el controlador de almacenamiento PV elija si desea distribuir o no la finalización de E/S.

1. Conectarse a la instancia mediante RDP
2. Abra un nuevo símbolo del sistema de PowerShell como administrador.
3. Ejecute el siguiente comando para establecer la clave de registro `NotiferDistributed`:

```
Set-ItemProperty -Type DWORD -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Value 0x00000001 -Name NotifierDistributed
```

4. Reinicie su instancia.

Distribuir tanto la preparación como la finalización

Establecer las claves de registro `NotifierDistributed` y `DpcRedirection` para distribuir siempre las fases de preparación y finalización.

1. Conectarse a la instancia mediante RDP
2. Abra un nuevo símbolo del sistema de PowerShell como administrador.
3. Ejecute los siguientes comandos para establecer las claves de registro `NotifierDistributed` y `DpcRedirection`.

```
Set-ItemProperty -Type DWORD -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Value 0x00000002 -Name NotifierDistributed
```

```
Set-ItemProperty -Type DWORD -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Value 0x00000001 -Name DpcRedirection
```

4. Reinicie su instancia.

Controladores NVMe de AWS para instancias de Windows

Los volúmenes de Amazon EBS y los volúmenes del almacén de instancias se exponen como dispositivos de bloques NVMe en instancias integradas en el AWS Nitro System. Para aprovechar al máximo el rendimiento y las capacidades de las características de Amazon EBS para los volúmenes expuestos como dispositivos de bloques NVMe, la instancia debe tener instalado el controlador AWS NVMe. Todas las AMI de AWS Windows de la generación actual vienen con el controlador AWS NVMe instalado de forma predeterminada.

Para obtener más información sobre EBS y NVMe, consulte Amazon EBS y NVMe en la Guía del usuario de Amazon EBS. Para obtener más información acerca del almacén de instancias de SSD y NVMe, consulte Volúmenes de almacén de instancias SSD.

Instalar o actualizar controladores NVMe de AWS mediante PowerShell

Si no está utilizando las AMI de Windows de AWS proporcionadas por Amazon, realice el procedimiento siguiente para instalar el controlador NVMe de AWS actual. Debería realizar esta actualización cuando sea adecuado reiniciar la instancia. O bien el script de instalación reiniciará la instancia o deberá hacerlo usted en la última etapa.

Requisitos previos

PowerShell 3.0 o posterior

Para descargar e instalar el controlador NVMe de AWS más reciente

1. Te recomendamos crear una AMI como copia de seguridad de la siguiente manera, en caso de que necesites revertir los cambios.

    a. Cuando detiene una instancia, se borran los datos contenidos en todos los volúmenes de almacén de instancias. Antes de detener una instancia, compruebe que ha copiado los datos que necesita de los volúmenes de almacén de instancias al almacenamiento persistente, como Amazon EBS o Amazon S3.
    b. En el panel de navegación, elija Instances (Instancias).
    c. Selecciona la instancia que requiere la actualización del controlador, selecciona Estado de instancia y a continuación selecciona Detener instancia.
    d. Una vez detenida la instancia, selecciona la instancia, selecciona Acciones, luego selecciona Imagen y plantillas y a continuación selecciona Crear imagen.
    e. Elija Instance state (Estado de la instancia) y Start instance (Iniciar instancia).

2. Conéctese a la instancia e inicie sesión como administrador local.
3. Descargue y extraiga los controladores en la instancia usando una de las siguientes opciones:
   - Uso de un navegador:
     a. Descargue el último paquete del controlador en la instancia.
     b. Extraiga el archivo zip.
   - Uso de PowerShell:

```
Invoke-WebRequest https://s3.amazonaws.com/ec2-windows-drivers-downloads/NVMe/
Latest/AWSNVMe.zip -outfile $env:USERPROFILE\nvme_driver.zip
Expand-Archive $env:userprofile\nvme_driver.zip -DestinationPath
 $env:userprofile\nvme_driver
```

> **Note**
>
> Si recibe un error al descargar el archivo y está usando Windows Server 2016 o una versión anterior, es posible que sea necesario habilitar TLS 1.2 para su terminal PowerShell. Puede habilitar TLS 1.2 para la sesión actual de PowerShell con el siguiente comando y luego volver a intentarlo:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol =
>  [Net.SecurityProtocolType]::Tls12
> ```

4. Instale el controlador en la instancia ejecutando el script PowerShell `install.ps1` desde el directorio `nvme_driver` (`.\install.ps1`). Si aparece un error, asegúrese de que está utilizando PowerShell 3.0 o posterior.

   a. (Opcional) A partir de la versión `1.5.0` de NVMe de AWS, se admiten las reservas persistentes de la interfaz de sistema informáticos pequeños (SCSI) en Windows Server 2016 y versiones posteriores. Esta característica agrega compatibilidad con los clústeres de conmutación por error de Windows Server con almacenamiento compartido de Amazon EBS. De forma predeterminada, esta característica no está habilitada durante la instalación.

   Puede activar la característica al ejecutar el script `install.ps1` para instalar el controlador y especificar el parámetro `EnableSCSIPersistentReservations` con un valor de `$true`.

```
PS C:\> .\install.ps1 -EnableSCSIPersistentReservations $true
```

Puede deshabilitar la característica al ejecutar el script `install.ps1` para instalar el controlador y especificar el parámetro `EnableSCSIPersistentReservations` con un valor de `$false`.

```
PS C:\> .\install.ps1 -EnableSCSIPersistentReservations $false
```

b. A partir de NVMe `1.5.0` de AWS, el script `install.ps1` siempre instala la herramienta `ebsnvme-id` con el controlador.

   (Opcional) En el caso de las versiones `1.4.0`, `1.4.1` y `1.4.2`, el script `install.ps1` permite especificar si la herramienta `ebsnvme-id` debe instalarse con el controlador.

   i. Para instalar la herramienta `ebsnvme-id`, especifique `InstallEBSNVMeIdTool 'Yes'`.

   ii. Si no desea instalar la herramienta, especifique `InstallEBSNVMeIdTool 'No'`.

   Si no se especifica `InstallEBSNVMeIdTool` y la herramienta ya está presente en `C:\ProgramData\Amazon\Tools`, el paquete actualizará la herramienta de forma predeterminada. Si la herramienta no está presente, `install.ps1` no actualizará la herramienta de forma predeterminada.

   Si no desea instalar la herramienta como parte del paquete, sino más adelante, puede encontrar la última versión o la herramienta en el paquete de controladores. Como alternativa, puede descargar la versión `1.0.0` desde Amazon S3:

   Descargue la herramienta `ebsnvme-id`.

5. Si el instalador no reinicia la instancia automáticamente, reiníciela.

Instalación o actualización de controladores NVMe de AWS con el Distribuidor

Puede usar el Distribuidor, una capacidad de AWS Systems Manager, para instalar el paquete de controladores NVMe una vez, o con actualizaciones programadas.

1. Para obtener instrucciones sobre cómo instalar el paquete de controladores NVMe mediante el Distribuidor, consulte los procedimientos en Instalar o actualizar paquetes en la Guía del usuario de Amazon EC2 Systems Manager.
2. En Nombre, elija AWSNVMe.
3. En Tipo de instalación, seleccione Desinstalar y volver a instalar
4. (Opcional) Personalice la instalación al especificar los valores para `AdditionalArguments`.

   a. A partir de NVMe `1.5.0` de AWS, el controlador admite las reservas persistentes de SCSI para Windows Server 2016 y versiones posteriores. De forma predeterminada, esta característica no está habilitada durante la instalación. Para habilitar esta característica, especifique `{"SSM_EnableSCSIPersistentReservations": $true}` para `AdditionalArguments`. Si no desea habilitar esta característica, especifique `{"SSM_EnableSCSIPersistentReservations": $false}` para `AdditionalArguments`.

   b. A partir de NVMe `1.5.0` de AWS, el script `install.ps1` siempre instalará la herramienta `ebsnvme-id`.

      (Opcional) En el caso de las versiones `1.4.0`, `1.4.1` y `1.4.2`, el script `install.ps1` permite especificar si la herramienta ebsnvme-id debe instalarse con el controlador.

      i. Para instalar la herramienta ebsnvme-id, especifique `{"SSM_InstallEBSNVMeIdTool": "Yes"}` para `AdditionalArguments`.

      ii. Si no desea instalar la herramienta, especifique `{"SSM_InstallEBSNVMeIdTool": "No"}` para `AdditionalArguments`.

      Si no se especifica `SSM_InstallEBSNVMeIdTool` para `AdditionalArguments` y la herramienta ya está presente en `C:\ProgramData\Amazon\Tools`, el paquete actualizará la herramienta de forma predeterminada. Si la herramienta no está presente, el paquete no actualizará la herramienta de forma predeterminada. Argumentos adicionales debe formatearse con una sintaxis JSON válida. Para ver ejemplos de cómo pasar argumentos adicionales para el paquete `aws configure`, consulte la documentación de Amazon EC2 Systems Manager.

      Si no desea instalar la herramienta como parte del paquete, sino más adelante, puede encontrar la última versión de la herramienta en el paquete de controladores. Como alternativa, puede descargar la versión `1.0.0` desde Amazon S3:

Descargue la herramienta `ebsnvme-id`.

5. Si el instalador no reinicia la instancia automáticamente, reiníciela.

Configure las reservas persistentes de SCSI

Una vez instalada la versión `1.5.0` o posterior del controlador de NVMe de AWS, puede habilitar o deshabilitar las reservas persistentes SCSI mediante el registro de Windows para Windows Server 2016 y versiones posteriores. Debe reiniciar la instancia para que estos cambios en el registro surjan efecto.

Puede habilitar las reservas persistentes de SCSI con el siguiente comando, que establece el `EnableSCSIPersistentReservations` en un valor de `1`.

```
PS C:\> $registryPath = "HKLM:\SYSTEM\CurrentControlSet\Services\AWSNVMe\Parameters
\Device"
Set-ItemProperty -Path $registryPath -Name EnableSCSIPersistentReservations -Value 1
```

Puede deshabilitar las reservas persistentes de SCSI con el siguiente comando, que establece el `EnableSCSIPersistentReservations` en un valor de `0`.

```
PS C:\> $registryPath = "HKLM:\SYSTEM\CurrentControlSet\Services\AWSNVMe\Parameters
\Device"
Set-ItemProperty -Path $registryPath -Name EnableSCSIPersistentReservations -Value 0
```

Historial de versiones de los controladores NVMe de AWS

En la siguiente tabla se describen las versiones del controlador NVMe de AWS.

Versión de paquete	Versión de controlador	Detalles	Fecha de la versión
1.5.1	1.5.0	Se corrigió el script de instalación para crear una carpeta para la herramienta ebsnvme-id si no estaba presente.	17 de noviembre de 2023
1.5.0	1.5.0	Se agregó compatibilidad con las reservas persistentes de la Interfaz de sistemas informáticos pequeños (SCSI) para las instancias que ejecutan Windows	31 de agosto de 2023

Versión de paquete	Versión de controlador	Detalles	Fecha de la versión
		Server 2016 y versiones posteriores. La herramienta ebsnvme-id (`ebsnvme-id.exe`) ahora está instalada de forma predeterminada.	
1.4.2	1.4.2	Se ha corregido un error que provocaba que Controlador NVMe de AWS no admitiera los volúmenes del almacén de instancias en las instancias de D3.	16 de marzo de 2023
1.4.1	1.4.1	Informes de escritura preferida del espacio de nombres con un alto grado de detalle (NPGW) para volúmenes de EBS que admiten esta característica opcional de NVMe. Para obtener más información, consulte la sección 8.25, “Improving Performance through I/O Size and Alignment Adherence” (Mejora del rendimiento a través de E/S y el cumplimiento de la alineación), en la Especificación base de NVMe, versión 1.4.	20 de mayo de 2022

Versión de paquete	Versión de controlador	Detalles	Fecha de la versión
1.4.0	1.4.0	• Se ha agregado soporte para IOCTL que permite a las aplicaciones interactuar con dispositivos NVMe. Este soporte permite que las aplicaciones obtengan la lista de `IdentifyController` ,`IdentifyNamespace` y `NameSpace` del dispositivo NVMe. Para obtener más información, consulte Consultas específicas del protocolo en la documentación de Microsoft. • La instalación de AWSNVMe 1.4.0 en Windows Server 2008 R2 producirá un error. La versión 1.3.2 y anteriores de AWSNVMe son compatibles con Windows Server 2008 R2. • La versión del controlador 1.4.0 y la última herramienta `ebsnvme-id` (`ebsnvme-id.exe`) se combinan en un solo paquete. Esta combinación le permite instalar el controlador y la herramienta desde un solo paquete. Para obtener más información, consulte Instalar o actualizar controladores NVMe de AWS mediante PowerShell. • Correcciones de errores y mejoras de fiabilidad.	23 de noviembre de 2021
1.3.2	1.3.2	Se ha corregido un problema en la modificación de volúmenes de EBS que procesaban de forma activa E/S, lo que podría dar lugar a daños en los datos. Los clientes que no modifican volúmenes de EBS online (por ejemplo, cambiando el tamaño o el tipo) no se ven afectados.	10 de septiembre de 2019

Versión de paquete	Versión de controlador	Detalles	Fecha de la versión
1.3.1	1.3.1	Mejoras de fiabilidad.	21 de mayo de 2019
1.3.0	1.3.0	Mejoras en la optimización del dispositivo.	31 de agosto de 2018
1.2.0	1.2.0	Mejoras de rendimiento y fiabilidad de los dispositivos NVMe de AWS en todas las instancias admitidas, incluidas las instancias bare metal.	13 de junio de 2018
1.0.0	1.0.0	Controlador NVMe de AWS para los tipos de instancias admitidos que ejecutan Windows Server.	12 de febrero de 2018

Suscribirse a las notificaciones de

Amazon SNS puede notificarle cuando se publiquen nuevas versiones de los controladores de Windows para EC2. Para suscribirse a estas notificaciones, utilice el siguiente procedimiento.

Para suscribirse a las notificaciones de EC2 desde la consola

1. Abra la consola de Amazon SNS en https://console.aws.amazon.com/sns/v3/home.
2. En la barra de navegación, cambie la región a EE. UU. Este (Norte de Virginia), si es necesario. Debe seleccionar esta región porque las notificaciones de SNS a las que se va a suscribir están en esa región.
3. En el panel de navegación, seleccione Subscriptions.
4. Seleccione Create subscription.
5. En el cuadro de diálogo Crear suscripción, haga lo siguiente:
   a. En ARN de tema, copie el siguiente nombre de recurso de Amazon (ARN):

      arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers

b. En Protocol (Protocolo), elija `Email`.

c. En Punto de conexión, escriba una dirección de correo electrónico que pueda utilizar para recibir notificaciones.

d. Seleccione Create subscription.

6. Debe recibir un correo electrónico de confirmación. Abra el mensaje y siga las instrucciones para completar la suscripción.

Cuando se publican nuevos controladores de Windows para EC2, enviamos notificaciones a los suscriptores. Si ya no desea recibir estas notificaciones, utilice el siguiente procedimiento para cancelar la suscripción.

Para anular la suscripción a las notificaciones del controlador de Windows para Amazon EC2

1. Abra la consola de Amazon SNS en https://console.aws.amazon.com/sns/v3/home.
2. En el panel de navegación, seleccione Subscriptions.
3. Seleccione la casilla de verificación de la suscripción y, a continuación, elija Acciones, Eliminar suscripciones. Cuando se le pida confirmación, seleccione Delete (Eliminar).

Para suscribirte a las notificaciones de EC2 utilizando AWS CLI

Para suscribirte a las notificaciones de EC2 con AWS CLI, utiliza el siguiente comando.

```
aws sns subscribe --topic-arn arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers --
protocol email --notification-endpoint YourUserName@YourDomainName.ext
```

Para suscribirse a las notificaciones de EC2 mediante AWS Tools for Windows PowerShell

Para suscribirte a las notificaciones de EC2 con AWS Tools for Windows PowerShell, utiliza el siguiente comando.

```
Connect-SNSNotification -TopicArn 'arn:aws:sns:us-east-1:801119661308:ec2-windows-
drivers' -Protocol email -Region us-east-1 -Endpoint 'YourUserName@YourDomainName.ext'
```

Configurar la instancia de Windows

Tras iniciar una instancia de Windows, puede iniciar sesión como administrador para realizar una configuración adicional de los agentes de inicialización y las características específicas de Windows. Los siguientes temas se centran en la configuración de instancias de Windows.

Contenido

Configuración de la inicialización de instancias de Windows de Amazon EC2

El agente de inicialización de Amazon EC2 realiza tareas durante el inicio de la instancia y se ejecuta si una instancia se detiene y posteriormente se inicia o se reinicia. Para obtener información sobre un agente específico, consulte las páginas de detalles de la siguiente lista.

- Configurar una instancia de Windows mediante EC2Launch v2
- Configurar una instancia de Windows utilizando EC2Launch
- Configuración de una instancia de Windows mediante el servicio EC2Config (heredado)

Contenidos

Comparación de los agentes de inicialización de Amazon EC2

La siguiente tabla muestra las principales diferencias de funcionalidad entre EC2Config, EC2Launch v1 y EC2Launch v2.

Característica	EC2Config	EC2Launch v1	EC2Launch v2
Run as (Ejecutar como)	Servicio de Windows	Scripts de PowerShell	Servicio de Windows
Admite	Solo sistema operativo heredado	Windows 2016 Windows 2019 (LTSC y SAC)	Windows 2016 Windows 2019 (LTSC y SAC) Windows 2022
Archivo de configuración	XML	XML	YAML
Establecer el nombre de usuario del administrador	No	No	Sí
Tamaño de los datos de usuario	16 KB	16 KB	60 KB (comprimido)
Datos de usuario local procesados en AMI	No	No	Sí, se puede configurar
Configuración de tareas en datos de usuario	No	No	Sí
Fondo de pantalla configurable	No	No	Sí
Personalizar el orden de ejecución de las tareas	No	No	Sí
Tareas configurables	15	9	20 durante la inicialización

Característica	EC2Config	EC2Launch v1	EC2Launch v2
Admite el Visor de eventos de Windows	Sí	No	Sí
Número de tipos de eventos del Visor de eventos	2	0	30

> **Note**
>
> La documentación de EC2Config se proporciona únicamente como referencia histórica. Microsoft ya no admite las versiones del sistema operativo en las que se ejecuta. Recomendamos encarecidamente que actualice al servicio de lanzamiento más reciente.

Configuración del sufijo de DNS para los agentes de inicialización de Windows

Con los agentes de inicialización de Amazon EC2, puede configurar una lista de sufijos de DNS que las instancias de Windows utilizan para la resolución de nombres de dominio. Los agentes de inicialización anulan la configuración estándar de Windows en la clave de registro `System\CurrentControlSet\Services\Tcpip\Parameters\SearchList` al agregar los siguientes valores a la lista de búsqueda de sufijos de DNS:

- El dominio de la instancia
- Los sufijos que resultan de la devolución del dominio de la instancia
- Dominio NV
- Los dominios especificados por cada tarjeta de interfaz de red

Todos los agentes de inicialización admiten la configuración de sufijos de DNS. Para obtener más información, consulte la versión específica del agente de inicialización:

- Para obtener información sobre la tarea `setDnsSuffix` y sobre cómo configurar los sufijos de DNS en EC2launch v2, consulte setDnsSuffix .
- Para obtener información sobre la configuración de la lista de sufijos de DNS y sobre cómo habilitar o deshabilitar la devolución en EC2launch v1, consulte Configurar EC2Launch.

- Para obtener información sobre la configuración de la lista de sufijos de DNS y sobre cómo habilitar o deshabilitar la devolución en EC2Config, consulte Archivos de configuración de EC2Config.

Devolución de nombres de dominio

La devolución de nombres de dominio es un comportamiento de Active Directory que permite a los equipos de un dominio secundario acceder a los recursos del dominio principal sin utilizar un nombre de dominio completo. De forma predeterminada, la devolución de nombres de dominio continúa hasta que solo queden dos nodos en la progresión del nombre de dominio.

Los agentes de inicialización transfieren el nombre de dominio si la instancia está conectada a un dominio y agregan los resultados a la lista de búsqueda de sufijos de DNS que se mantiene en la clave de registro **`System\CurrentControlSet\Services\Tcpip\Parameters\SearchList`**. Los agentes utilizan la configuración de las siguientes claves de registro para determinar el comportamiento de devolución.

- **`System\CurrentControlSet\Services\Tcpip\Parameters\UseDomainNameDevolution`**
  - Si no se establece, deshabilita la devolución.
  - Si se establece en `1`, habilita la devolución (valor predeterminado).
  - Si no se establece en `0`, deshabilita la devolución.
- **`System\CurrentControlSet\Services\Dnscache\Parameters\DomainNameDevolutionLevel`**
  - Si no se establece, utilice el nivel 2 (valor predeterminado).
  - Si se establece en `3` o un número mayor, utilice el valor para establecer el nivel.

Al deshabilitar la devolución o cambiar su configuración a un nivel superior, la clave de registro `System\CurrentControlSet\Services\Tcpip\Parameters\SearchList` seguirá conteniendo los sufijos que se agregaron anteriormente. Estos no se eliminan automáticamente. Puede actualizar la lista de manera manual o borrarla y dejar que su agente lleve a cabo el proceso de configuración de la nueva lista.

> **Note**
>
> Para borrar la lista de sufijos de DNS del registro, puede ejecutar el siguiente comando.

```
PS C:\> Invoke-CimMethod -ClassName Win32_NetworkAdapterConfiguration -
MethodName "SetDNSSuffixSearchOrder" -Arguments @{ DNSDomainSuffixSearchOrder =
 $null } | Out-Null
```

Ejemplos de devolución

En los siguientes ejemplos se muestra la progresión de los nombres de dominio a lo largo del proceso de devolución.

`corp.example.com`

- Progresa hasta `example.com`.

`locale.region.corp.example.com`

1. Progresa hasta `region.corp.example.com`.
2. Progresa hasta `corp.example.com`.
3. Progresa hasta `example.com`.

`locale.region.corp.example.com` con una configuración de `DomainNameDevolutionLevel=3`

1. Progresa hasta `region.corp.example.com`.
2. Progresa hasta `corp.example.com`. La progresión se detiene aquí, debido a la configuración del nivel.

Configurar una instancia de Windows mediante EC2Launch v2

Todas las instancias admitidas de Amazon EC2 en las que se ejecute Windows Server 2022 incluyen el agente de inicialización EC2Launch v2 (`EC2Launch.exe`) de manera predeterminada. También proporcionamos AMI de Windows Server 2016 y 2019 con EC2Launch v2 instalado como agente de inicialización predeterminado. Estas AMI se proporcionan de manera adicional a las AMI de Windows Server 2016 y 2019 que incluyen EC2Launch v1. Puede buscar AMI de Windows que incluyan EC2Launch v2 de manera predeterminada ingresando el siguiente prefijo en la búsqueda en la página AMIs de la consola de Amazon EC2: `EC2LaunchV2-Windows_Server-*`.

EC2Launch v2 realiza tareas durante el inicio de la instancia y se ejecuta si una instancia se detiene y posteriormente se inicia, o se reinicia. EC2Launch v2 también puede realizar tareas bajo demanda. Algunas de estas tareas se activan automáticamente, mientras que otras se deben activar manualmente. El servicio EC2Launch v2 admite todas las características de EC2Config y EC2Launch.

Este servicio utiliza un archivo de configuración para controlar su funcionamiento. Puede actualizar el archivo de configuración mediante una herramienta gráfica o editándolo directamente como un archivo .yml único (`agent-config.yml`). Los binarios de servicio se encuentran en el directorio `%ProgramFiles%\Amazon\EC2Launch`.

EC2Launch v2 publica registros de eventos de Windows para ayudarlo a solucionar errores y establecer desencadenadores. Para obtener más información, consulte Registros de eventos de Windows.

Sistemas operativos compatibles

- Windows Server 2022
- Windows Server 2019 (canal de servicio a largo plazo y canal semestral)
- Windows Server 2016

Contenido de la sección EC2Launch v2

- Información general sobre EC2Launch v2
- Instalar la versión más reciente de EC2Launch v2
- Migrar a EC2Launch v2
- Detener, reiniciar, eliminar o desinstalar EC2Launch v2
- Suscribirse a las notificaciones del servicio EC2Launch v2
- Configuración de EC2Launch v2
- Solucionar problemas de EC2Launch v2
- Historiales de versiones de EC2Launch v2

Información general sobre EC2Launch v2

EC2Launch v2 es un servicio que realiza tareas durante el arranque de la instancia y se ejecuta si una instancia se detiene y posteriormente se inicia, o se reinicia.

Temas generales

- Conceptos de EC2Launch v2
- Tareas de EC2Launch v2
- Telemetría

Para comparar las características de la versión del agente de inicialización, consulte Comparación de los agentes de inicialización de Amazon EC2.

Conceptos de EC2Launch v2

Es útil entender los siguientes conceptos al considerar EC2Launch v2.

Tarea

Puede invocar una tarea para que realice una acción en una instancia. Se pueden configurar las tareas en el archivo `agent-config.yml` o a través de los datos de usuario. Para obtener una lista de las tareas disponibles para EC2Launch v2, consulte Tareas de EC2Launch v2. Para obtener información y el esquema sobre la configuración de tareas, consulte Configuración de tareas de EC2Launch v2.

Escenario

Una etapa es una agrupación lógica de tareas que ejecuta el agente EC2Launch v2. Algunas tareas solo pueden ejecutarse en una etapa específica. Otras se pueden ejecutar en varias etapas. Al usar `agent-config.yml`, debe especificar una lista de etapas y una lista de tareas a ejecutar dentro de cada etapa.

El servicio ejecuta las etapas en el siguiente orden:

Fase 1: Iniciar

Fase 2: Red

Fase 3: PreReady

Windows está listo

Una vez finalizada la etapa de preparación previa, el servicio envía el mensaje `Windows is ready` a la consola Amazon EC2.

Etapa 4: PostReady

Los datos del usuario se ejecutan durante la etapa PostReady. Algunas versiones del script se ejecutan antes de la etapa PostReady del archivo `agent-config.yml` y otras después, de la siguiente manera:

Antes de `agent-config.yml`

- Datos de usuario de YAML versión 1.1
- Datos de usuario XML

Después de `agent-config.yml`

- Datos de usuario de YAML, versión 1.0 (versión antigua para compatibilidad con versiones anteriores)

Para ver etapas y tareas de ejemplo, consulte Ejemplo: `agent-config.yml`.

Cuando utilice datos de usuario, debe especificar una lista de tareas para que las ejecute el agente de inicialización. El escenario está implícito. Para ver tareas de ejemplo, consulte Ejemplo: datos de usuario.

EC2Launch v2 ejecuta la lista de tareas en el orden en que usted especifique en `agent-config.yml` y en los datos de usuario. Las etapas se ejecutan de forma secuencial. La siguiente etapa comienza una vez finalizada la anterior. Las tareas se ejecutan de forma secuencial.

Frecuencia

La frecuencia de las tareas determina cuándo deben ejecutarse las tareas, en función del contexto de arranque. La mayoría de las tareas solo tienen una frecuencia permitida. Puede especificar la frecuencia de las tareas de `executeScript`.

Verá las siguientes frecuencias en Configuración de tareas de EC2Launch v2.

- Una vez: la tarea se ejecuta una vez, cuando la AMI se ha arrancado por primera vez (Sysprep terminado).
- Siempre: la tarea se ejecuta cada vez que se ejecuta el agente de inicialización. El agente de inicialización se ejecuta cuando:
  - una instancia se inicia o se reinicia
  - el servicio EC2Launch se ejecuta
  - `EC2Launch.exe run` se invoca

agent-config

`agent-config` es un archivo que se encuentra en la carpeta de configuración de EC2Launch v2. Incluye configuración para las etapas de arranque, red, PreReady y PostReady. Este archivo se utiliza con el objetivo de especificar la configuración de la instancia para las tareas que deben ejecutarse cuando la AMI se arranca por primera vez o las veces siguientes.

De forma predeterminada, la instalación de EC2Launch v2 instala un archivo `agent-config` que incluye configuraciones recomendadas que se utilizan en AMI estándar de Amazon Windows. Puede actualizar el archivo de configuración para modificar la experiencia de arranque predeterminada de la AMI que EC2Launch v2 especifique.

Datos de usuario

Los datos de usuario son datos que se pueden configurar al iniciar una instancia. Puede actualizar los datos de usuario para cambiar dinámicamente el modo en que se configuran las AMI personalizadas o las AMI de inicio rápido. EC2Launch v2 admite una entrada de datos de usuario de 60 KB. Los datos de usuario incluyen sólo la etapa UserData y, por lo tanto, se ejecutan después del archivo `agent-config`. Puede introducir datos de usuario al iniciar una instancia utilizando el asistente de inicialización de instancias o modificar los datos de usuario desde la consola de EC2. Para obtener más información sobre el trabajo con datos de usuarios, consulte Cómo gestiona Amazon EC2 los datos de usuario de las instancias de Windows.

Tareas de EC2Launch v2

EC2Launch v2 puede realizar las siguientes tareas en cada arranque:

- Configure fondos de pantalla nuevos y personalizados opcionalmente en los que se representen información sobre la instancia.
- Establezca los atributos de la cuenta de administrador que se crea en el equipo local.
- Agregue sufijos de DNS a la lista de sufijos de búsqueda. Sólo se agregan a la lista los sufijos que aún no existen.
- Establezca las letras de unidad para los volúmenes adicionales y amplíelas para utilizar el espacio disponible.
- Escriba archivos desde la configuración en el disco.
- Ejecute los scripts especificados en el archivo de configuración de EC2Launch v2 o desde `user-data`. Los scripts de `user-data` pueden ser texto plano o comprimidos y proporcionarse en formato base64.

- Ejecute un programa con argumentos dados.
- Establecer el nombre del equipo.
- Enviar información de instancia a la consola de Amazon EC2.
- Envía la huella digital del certificado RDP a la consola de Amazon EC2.
- Ampliar dinámicamente la partición del sistema operativo para incluir cualquier espacio sin particionar.
- Ejecute los datos del usuario. Para obtener más información acerca de cómo especificar datos de usuario, consulte Configuración de tareas de EC2Launch v2.
- Establezca rutas estáticas no persistentes para alcanzar el servicio de metadatos y los servidores AWS KMS.
- Establezca las particiones que no sean de arranque en `mbr` o `gpt`.
- Inicie el servicio Systems Manager tras Sysprep.
- Optimice la configuración de ENA.
- Habilite OpenSSH para versiones posteriores de Windows.
- Habilite tramas gigantes.
- Establezca Sysprep para que se ejecute con EC2Launch v2.
- Publique registros de eventos de Windows.

Telemetría

La telemetría es información adicional que ayuda a AWS a comprender mejor sus requisitos, diagnosticar problemas y ofrecer recursos para mejorar su experiencia con Servicios de AWS.

EC2Launch v2 versión `2.0.592` y posteriores recopilan telemetría, como métricas de uso y errores. Estos datos se recopilan de la instancia de Amazon EC2 en la que se ejecuta EC2Launch v2. Esto incluye todas las AMI de Windows que son propiedad de AWS.

EC2Launch v2 recopila los siguientes tipos de telemetría:

- Información de uso: comandos del agente, método de instalación y frecuencia de ejecución programada.
- Errores e información de diagnóstico: códigos de error de instalación del agente, códigos de error de ejecución y pilas de llamadas con error.

Ejemplos de datos recopilados:

```
2021/07/15 21:44:12Z: EC2LaunchTelemetry: IsAgentScheduledPerBoot=true
2021/07/15 21:44:12Z: EC2LaunchTelemetry: IsUserDataScheduledPerBoot=true
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentCommandCode=1
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentCommandErrorCode=5
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentInstallCode=2
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentInstallErrorCode=0
```

La telemetría se encuentra habilitada de forma predeterminada. Puede desactivar la recopilación de telemetría en cualquier momento. Si la telemetría se encuentra habilitada, EC2Launch v2 envía datos de telemetría sin notificaciones adicionales de los clientes.

Visibilidad de telemetría

Cuando la telemetría se encuentra habilitada, aparece en el resultado de la consola de Amazon EC2 de la siguiente manera.

```
2021/07/15 21:44:12Z: Telemetry: <Data>
```

Desactivar la telemetría en una instancia

Para desactivar la telemetría en una sola instancia, puede definir una variable de entorno del sistema o utilizar el MSI a fin de modificar la instalación.

Para desactivar la telemetría al establecer una variable de entorno de sistema, ejecute el siguiente comando como administrador.

```
setx /M EC2LAUNCH_TELEMETRY 0
```

Para desactivar la telemetría mediante el MSI, ejecute el siguiente comando después de descargar el MSI.

```
msiexec /i ".\AmazonEC2Launch.msi" Remove="Telemetry" /q
```

Instalar la versión más reciente de EC2Launch v2

Puede utilizar uno de los siguientes métodos para instalar el agente EC2Launch v2 en su instancia de EC2:

- Descargue el agente de Amazon S3 e instálelo con Windows PowerShell. Para obtener URL de descargas, consulte Descargas de EC2Launch v2 en Amazon S3.

- Instale desde SSM Distributor.
- Instale desde un componente de EC2 Image Builder.
- Lance la instancia desde una AMI que tenga EC2Launch v2 preinstalado.

> **Warning**
>
> AmazonEC2Launch.msi desinstala versiones anteriores de los servicios de inicialización de EC2, como EC2Launch (v1) y EC2Config.

Para ver los pasos de instalación, seleccione la pestaña que coincida con su método preferido.

Windows PowerShell

Para instalar la versión más reciente del agente EC2Launch v2 con Windows PowerShell, siga estos pasos.

1. Cree su directorio local.

```
New-Item -Path "$env:USERPROFILE\Desktop\EC2Launchv2" -ItemType Directory
```

2. Configure la URL de la ubicación de descarga. Ejecute el siguiente comando con la URL de Amazon S3 que utilizará. Para obtener URL de descargas, consulte Descargas de EC2Launch v2 en Amazon S3

```
$Url = "Amazon S3 URL/AmazonEC2Launch.msi"
```

3. Utilice el siguiente comando compuesto para descargar el agente y ejecutar la instalación

```
$DownloadFile = "$env:USERPROFILE\Desktop\EC2Launchv2\" + $(Split-Path -Path
 $Url -Leaf)
Invoke-WebRequest -Uri $Url -OutFile $DownloadFile
msiexec /i "$DownloadFile"
```

> **Note**
>
> Si recibe un error al descargar el archivo y está usando Windows Server 2016 o una versión anterior, es posible que sea necesario habilitar TLS 1.2 para su terminal

PowerShell. Puede habilitar TLS 1.2 para la sesión actual de PowerShell con el siguiente comando y luego volver a intentarlo:

```
[Net.ServicePointManager]::SecurityProtocol =
 [Net.SecurityProtocolType]::Tls12
```

4. Para comprobar la instalación, compruebe que el archivo msi existe en el directorio EC2Launch v2 de su instancia (`C:\ProgramData\Amazon\EC2Launch`).

AWS Systems Manager Distributor

Para configurar las actualizaciones automáticas de EC2launch v2 con configuración AWS Systems Manager rápida, consulte Instale y actualice de forma automática con la configuración rápida del distribuidor..

También puede realizar una instalación única del `AWSEC2Launch-Agent` paquete desde AWS Systems Manager Distributor. Para obtener instrucciones sobre cómo instalar un paquete desde Systems Manager Distributor, consulte Instalar o actualizar paquetes en la Guía del usuario de AWS Systems Manager.

EC2 Image Builder component

Puede instalar el componente `ec2launch-v2-windows` cuando crea una imagen personalizada con EC2 Image Builder. Para obtener instrucciones sobre cómo crear una imagen personalizada con EC2 Image Builder, consulteCreación de una canalización de imágenes utilizando el asistente de consola de EC2 Image Builder en la Guía del usuario de EC2 Image Builder.

AMI

EC2Launch v2 está preinstalado de forma predeterminada en las siguientes AMI de Windows Server 2022 y las AMI de UEFI:

- Windows_Server-2022-English-Full-Base
- Windows_Server-2022-English-Core-Base
- AMI de Windows Server 2022 con todos los demás idiomas
- AMI de Windows Server 2022 con SQL instalado
- Windows_Server-2022-English-Core-EKS_Optimized

EC2Launch v2 también está preinstalado en las siguientes AMI de Windows Server. Puede encontrar estas AMI en la consola de Amazon EC2 o utilizando el siguiente prefijo de búsqueda: `EC2LaunchV2-` en la AWS CLI.

- EC2LaunchV2-Windows_Server-2019-English-Core-Base
- EC2LaunchV2-Windows_Server-2019-English-Full-Base
- EC2LaunchV2-Windows_Server-2016-English-Core-Base
- EC2LaunchV2-Windows_Server-2016-English-Full-Base
- EC2LaunchV2-Windows_Server-2012_R2_RTM-English-Full-Base
- EC2LaunchV2-Windows_Server-2012_RTM-English-Full-Base

Instale y actualice EC2Launch v2 de forma automática con la configuración rápida del distribuidor de AWS Systems Manager.

Con la configuración rápida del distribuidor de AWS Systems Manager, puede configurar actualizaciones automáticas para EC2launch v2. El siguiente proceso configura una Asociación de Systems Manager en la instancia que actualiza automáticamente el agente EC2Launch v2 con la frecuencia que especifique. La asociación que crea la configuración rápida del distribuidor puede incluir instancias de una región y Cuenta de AWS, o instancias de una organización AWS. Para obtener más información sobre cómo crear una organización, consulte Tutorial: Creación y configuración de una organización en la AWS OrganizationsGuía del usuario.

Antes de comenzar, asegúrese de que las instancias cumplen todos los requisitos previos.

Requisitos previos

Para configurar las actualizaciones automáticas con la configuración rápida del distribuidor, las instancias deben cumplir los siguientes requisitos previos.

- Tiene al menos una instancia en ejecución que admite EC2Launch v2. Consulte los sistemas operativos admitidos por EC2Launch v2.
- Ha realizado las tareas de configuración de Systems Manager en sus instancias. Para obtener más información, consulte Configuración de Systems Manager en la AWS Systems ManagerGuía del usuario.
- EC2Launch v2 debe ser el único agente de lanzamiento instalado en su instancia. Si tiene más de un agente de lanzamiento instalado, la configuración rápida del distribuidor fallará. Antes de

configurar EC2Launch v2 con una configuración rápida del distribuidor, desinstale los agentes de lanzamiento de EC2Config o EC2Launch v1, si existen.

Cómo configurar la configuración rápida del distribuidor para EC2Launch v2

Para crear una configuración para EC2Launch v2 con la configuración rápida del distribuidor, utilice las siguientes configuraciones cuando complete los pasos para la implementación del paquete de distribuidor:

- Paquetes de software: Agente Amazon EC2Launch v2.
- Frecuencia de actualización: Seleccione una frecuencia de la lista.
- Objetivos: Elija entre las opciones de implementación disponibles.

Para comprobar el estado de la configuración, vaya a la pestaña Configuraciones de configuración rápida de Systems Manager en el AWS Management Console.

1. Abra la consola de AWS Systems Manager en https://console.aws.amazon.com/systems-manager/.
2. En el panel de navegación, elija Quick Setup.
3. En la pestaña Configuraciones, seleccione la fila asociada a la configuración que creó. La pestaña Configuraciones muestra las configuraciones e incluye un resumen de los detalles clave, como la región, el estado de la implementación y el estado de la asociación.

   > **Note**
   >
   > El nombre de la asociación de cada configuración de EC2Launch v2 Distributor comienza con el siguiente prefijo: `AWS-QuickSetup-Distributor-EC2Launch-Agent-`.

4. Para ver los detalles, seleccione la configuración y elija Ver detalles.

Para obtener más información y los pasos de solución de problemas, consulte los resultados de solución de problemas de la configuración rápida en la AWS Systems ManagerGuía del usuario.

Descargas de EC2Launch v2 en Amazon S3

Para instalar la versión más reciente de EC2Launch v2, descargue el instalador de una de las siguientes ubicaciones:

> **Note**
>
> El enlace de instalación de 32 bits quedará obsoleto. Le recomendamos que utilice el enlace de instalación de 64 bits para instalar EC2Launch v2. Si necesita un agente de inicialización de 32 bits, utilice EC2Config.

- 64 bits: https://s3.amazonaws.com/amazon-ec2launch-v2/windows/amd64/latest/AmazonEC2Launch.msi
- 32 bits: https://s3.amazonaws.com/amazon-ec2launch-v2/windows/386/latest/AmazonEC2Launch.msi

Configurar las opciones de instalación

Al instalar o actualizar EC2Launch v2, puede configurar las opciones de instalación con el cuadro de diálogo de instalación de EC2Launch v2 o con el comando msiexec en una consola de línea de intérprete de comandos.

La primera vez que el instalador de EC2Launch v2 se ejecuta en una instancia, inicializa la configuración del agente de inicialización de la instancia de la siguiente manera:

- Crea la ruta local y escribe en ella el archivo del agente de inicialización. Esto a veces se denomina instalación limpia.
- Crea la variable de entorno `EC2LAUNCH_TELEMETRY` si aún no existe, y la establece en función de su configuración.

Para obtener detalles de configuración, seleccione la pestaña que coincida con el método de configuración que utilizará.

Amazon EC2Launch Setup dialog

Al instalar o actualizar EC2Launch v2, puede configurar las siguientes opciones de instalación a través del cuadro de diálogo de instalación de EC2Launch v2.

Opciones de instalación básica

Enviar telemetría

Al incluir esta característica en el cuadro de diálogo de configuración, el instalador establece la variable de entorno `EC2LAUNCH_TELEMETRY` hasta un valor de `1`. Si deshabilita Enviar telemetría, el instalador establece la variable de entorno en un valor de `0`.

Cuando se ejecuta el agente EC2Launch v2, lee la variable de entorno `EC2LAUNCH_TELEMETRY` para determinar si se deben cargar datos de telemetría. Si el valor es igual a `1`, carga los datos. De lo contrario, no los carga.

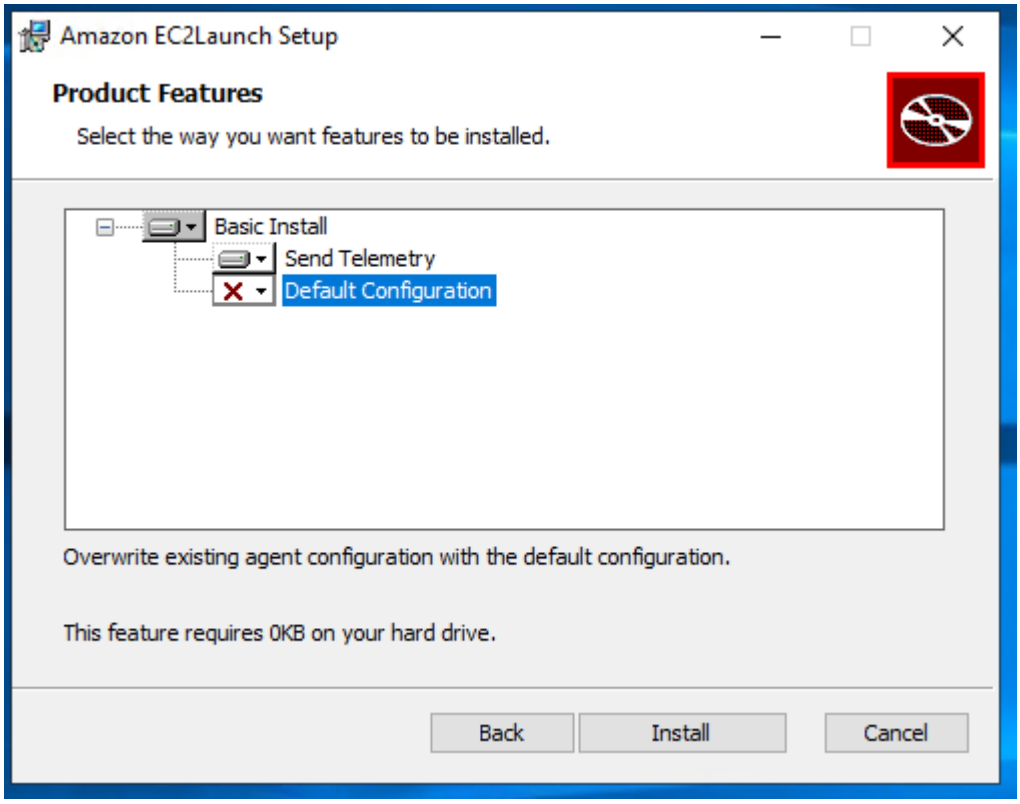
Configuración predeterminada

La configuración predeterminada de EC2Launch v2 consiste en sobrescribir el agente de inicialización local si ya existe. La primera vez que ejecuta una instalación en una instancia, la configuración predeterminada realiza una instalación limpia. Si deshabilita la configuración predeterminada en la instalación inicial, se producirá un error en la instalación.

Si vuelve a ejecutar la instalación en la instancia, puede deshabilitar la configuración predeterminada para realizar una actualización que no sustituya el archivo `%ProgramData%/Amazon/EC2Launch/config/agent-config.yml`.

Ejemplo: actualizar EC2Launch v2 con telemetría

El siguiente ejemplo muestra el cuadro de diálogo de configuración de EC2Launch v2 configurado para actualizar la instalación actual y habilitar la telemetría. Esta configuración realiza una instalación sin reemplazar el archivo de configuración del agente y establece la variable de entorno `EC2LAUNCH_TELEMETRY` hasta un valor de `1`.



Command line

Al instalar o actualizar EC2Launch v2, puede configurar las siguientes opciones de instalación con el comando msiexec en una consola de línea de intérprete de comandos.

Valores de parámetro **`ADDLOCAL`**

Básico (obligatorio)

Instale el agente de inicialización. Si este valor no está presente en el parámetro `ADDLOCAL`, finaliza la instalación.

Limpio

Cuando incluye el valor `Clean` en el parámetro `ADDLOCAL`, el instalador escribe el archivo de configuración del agente en la siguiente ubicación: `%ProgramData%/Amazon/EC2Launch/config/agent-config.yml`. Si el archivo de configuración del agente ya existe, lo sobrescribe.

Cuando salga del valor `Clean` fuera del parámetro `ADDLOCAL`, el instalador realiza una actualización que no reemplaza el archivo de configuración del agente.

Telemetría

Cuando incluye el valor `Telemetry` en el parámetro `ADDLOCAL`, el instalador establece loa variable de entrono `EC2LAUNCH_TELEMETRY` hasta un valor de `1`.

Cuando salga del valor `Telemetry` fuera del parámetro `ADDLOCAL`, el instalador establece la variable de entorno en un valor de `0`.

Cuando se ejecuta el agente EC2Launch v2, lee la variable de entorno `EC2LAUNCH_TELEMETRY` para determinar si se deben cargar datos de telemetría. Si el valor es igual a `1`, carga los datos. De lo contrario, no los carga.

Ejemplo: instalar EC2Launch v2 con telemetría

```
& msiexec /i "C:\Users\Administrator\Desktop\EC2Launchv2\AmazonEC2Launch.msi"
 ADDLOCAL="Basic,Clean,Telemetry" /q
```

Verificar la versión de EC2Launch v2

Siga uno de los procedimientos siguientes para verificar la versión de EC2Launch v2 instalada en las instancias.

Windows PowerShell

Verifique la versión instalada de EC2Launch v2 con Windows PowerShell de la siguiente manera.

1. Lance una instancia desde la AMI y conéctese a ella.
2. Ejecute el siguiente comando en PowerShell para verificar la versión instalada de EC2Launch v2:

   ```
   & "C:\Program Files\Amazon\EC2Launch\EC2Launch.exe" version
   ```

Windows Control Panel

Verifique la versión instalada de EC2Launch v2 en el panel de control de Windows de la siguiente manera.

1. Lance una instancia desde la AMI y conéctese a ella.

2. Abra el panel de control de Windows y elija Programas y características.
3. En la lista de programas instalados, busque `Amazon EC2Launch`. Su número de versión aparece en la columna Version (Versión).

Para ver las actualizaciones más recientes de las AMI de Windows de AWS, consulte el historial de versiones de las AMI de Windows en la Referencia de las AMI de Windows de AWS.

Para obtener la última versión de EC2Launch v2, consulte Historial de versiones de EC2Launch v2.

Para obtener la versión más reciente de la herramienta de migración de EC2Launch v2, consulte Historial de versiones de la herramienta de migración de EC2Launch v2.

Puede recibir notificaciones cuando se publiquen nuevas versiones del servicio EC2Launch v2. Para obtener más información, consulte Suscribirse a las notificaciones del servicio EC2Launch v2.

Migrar a EC2Launch v2

La herramienta de migración EC2Launch actualiza el agente de inicialización instalado (EC2Config y EC2Launch v1) desinstalándolo e instalando EC2Launch v2. Las configuraciones aplicables de los servicios de inicialización anteriores se migran automáticamente al nuevo servicio. La herramienta de migración no detecta ninguna tarea programada que esté vinculada a scripts de EC2Launch v1; por lo tanto, no configura automáticamente dichas tareas en EC2Launch v2. Para configurar dichas tareas, edita el archivo `agent-config.yml` o utiliza el Cuadro de diálogo configuración de EC2Launch v2. Por ejemplo, si una instancia tiene una tarea programada que ejecuta `InitializeDisks.ps1`, después de ejecutar la herramienta de migración debe especificar los volúmenes que desea iniciar en el cuadro de diálogo configuración de EC2Launch v2. Consulte el paso 6 del procedimiento para Cambiar la configuración mediante el cuadro de diálogo de configuración de EC2Launch v2.

Puede descargar la herramienta de migración o instalarla con un documento de SSM RunCommand.

Puede descargar la herramienta desde las siguientes ubicaciones:

> **Note**
>
> El enlace de la herramienta de migración de 32 bits quedará obsoleto. Le recomendamos que utilice el enlace de 64 bits para migrar a EC2Launch v2. Si necesita un agente de inicialización de 32 bits, utilice EC2Config.

- 64 bits: https://s3.amazonaws.com/amazon-ec2launch-v2-utils/MigrationTool/windows/amd64/latest/EC2LaunchMigrationTool.zip
- 32 bits: https://s3.amazonaws.com/amazon-ec2launch-v2-utils/MigrationTool/windows/386/latest/EC2LaunchMigrationTool.zip

> **Note**
>
> Debe ejecutar la herramienta de migración EC2Launch v2 como administrador. EC2Launch v2 se instala como un servicio después de ejecutar la herramienta de migración. No se ejecuta inmediatamente. De forma predeterminada, se ejecuta durante el inicio de la instancia y se ejecuta si una instancia se detiene y se inicia o se reinicia posteriormente.

Utilice el documento de SSM `AWSEC2Launch-RunMigration` para migrar a la versión de EC2Launch v2 más reciente con SSM Run Command. El documento no requiere ningún parámetro. Para obtener más información sobre el uso de SSM Run Command, consulte Systems Manager Run Command de AWS.

La herramienta de migración aplica las siguientes configuraciones de EC2Config a EC2Launch v2.

- Si `Ec2DynamicBootVolumeSize` se configura como `false`, se elimina la etapa `boot` de EC2Launch v2
- Si `Ec2SetPassword` se configura como `Enabled`, el tipo de contraseña de EC2Launch v2 se configura como `random`
- Si `Ec2SetPassword` se configura como `Disabled`, el tipo de contraseña de EC2Launch v2 se configura como `donothing`
- Si `SetDnsSuffixList` se configura como `false`, se elimina la tarea `setDnsSuffix` de EC2Launch v2
- Si `EC2SetComputerName` se configura como verdadero, se agrega la tarea `setHostName` de EC2Launch v2 a la configuración `yaml`

La herramienta de migración aplica las siguientes configuraciones de EC2Launch v1 a EC2Launch v2.

- Si `ExtendBootVolumeSize` se configura como `false`, se elimina la etapa `boot` de EC2Launch v2

- Si `AdminPasswordType` se configura como `Random`, el tipo de contraseña de EC2Launch v2 se configura como `random`
- Si `AdminPasswordType` se establece como `Specify`, el tipo de contraseña EC2Launch v2 se establece como `static` y los datos de contraseña como la contraseña especificada en `AdminPassword`
- Si `SetWallpaper` se configura como `false`, se elimina la tarea `setWallpaper` de EC2Launch v2
- Si `AddDnsSuffixList` se configura como `false`, se elimina la tarea `setDnsSuffix` de EC2Launch v2
- Si `SetComputerName` se establece como `true`, se agrega la tarea de EC2Launch v2 `setHostName`

Detener, reiniciar, eliminar o desinstalar EC2Launch v2

Puede administrar el servicio EC2Launch v2 tal cual lo haría con cualquier otro servicio de Windows.

EC2Launch v2 se ejecuta una vez en el arranque y ejecuta todas las tareas configuradas. Después de ejecutar tareas, el servicio entra en un estado detenido. Cuando reinicie el servicio, el servicio volverá a ejecutar todas las tareas configuradas y volverá a un estado detenido.

Para aplicar la configuración actualizada a la instancia, puede detener y reiniciar el servicio. Si está instalando EC2Launch v2 manualmente, primero debe detener el servicio.

Para detener el servicio EC2Launch v2

1. Lance y conéctese a la instancia de Windows.
2. En el menú Inicio elija Herramientas administrativas y, a continuación, abra Servicios.
3. En la lista de servicios, haga clic con el botón derecho en Amazon EC2Launch y seleccione Detener.

Para reiniciar el servicio EC2Launch v2

1. Lance y conéctese a la instancia de Windows.
2. En el menú Inicio elija Herramientas administrativas y, a continuación, abra Servicios.
3. En la lista de servicios, haga clic con el botón derecho en Amazon EC2Launch y seleccione Reiniciar.

Si no necesita actualizar las opciones de configuración, crear su propia AMI o utilizar AWS Systems Manager, puede eliminar y desinstalar el servicio. Si elimina un servicio, se eliminará su subclave de registro. La desinstalación de un servicio elimina los archivos, las subclaves de registro y cualquier acceso directo al servicio.

Para eliminar el servicio EC2Launch v2

1. Inicie una ventana del símbolo del sistema.
2. Ejecute el comando siguiente:

```
sc delete EC2Launch
```

Para desinstalar EC2Launch v2

1. Lance y conéctese a la instancia de Windows.
2. En el menú Start (Inicio), elija Control Panel (Panel de control).
3. Abra Programs (Programas) y, a continuación, Programs and Features (Programas y características).
4. En la lista de programas, elija Amazon EC2Launch. Para confirmar que elige v2, marque la columna Version (Versión).
5. Elija Desinstalar.

Suscribirse a las notificaciones del servicio EC2Launch v2

Amazon SNS puede enviarle notificaciones cuando se publiquen nuevas versiones del servicio EC2Launch v2. Para suscribirse a estas notificaciones, utilice el siguiente procedimiento.

Suscribirse a notificaciones de EC2Launch v2

1. Inicie sesión en AWS Management Console y abra la consola de Amazon SNS en https://console.aws.amazon.com/sns/v3/home.
2. En la barra de navegación, cambie la región a EE. UU. Este (Norte de Virginia), si es necesario. Debe seleccionar esta región porque las notificaciones de SNS a las que se va a suscribir se han creado en esa región.
3. En el panel de navegación, seleccione Subscriptions.
4. Seleccione Create subscription.

5. En el cuadro de diálogo Crear suscripción, haga lo siguiente:

    a. En ARN del tema, utilice el Nombre de recurso de Amazon (ARN) siguiente: arn:aws:sns:us-east-1:309726204594:amazon-ec2launch-v2.

    b. En Protocol (Protocolo), elija Email (Correo electrónico).

    c. En Punto de conexión, escriba una dirección de correo electrónico que pueda utilizar para recibir notificaciones.

    d. Seleccione Create subscription.

6. Recibirá un correo electrónico donde se solicita que confirme la suscripción. Abra el mensaje y siga las instrucciones para completar la suscripción.

Cada vez que se publique una nueva versión del servicio EC2Launch v2, enviaremos una notificación a los suscriptores. Si ya no desea recibir estas notificaciones, utilice el siguiente procedimiento para cancelar la suscripción.

1. Abra la consola de Amazon SNS.
2. En el panel de navegación, seleccione Subscriptions.
3. Seleccione la suscripción y, en Acciones, elija Delete subscriptions (Eliminar suscripciones). Cuando se le pida confirmación, seleccione Delete (Eliminar).

Configuración de EC2Launch v2

Esta sección contiene información acerca de cómo configurar las opciones para EC2Launch v2.

Los temas incluyen:

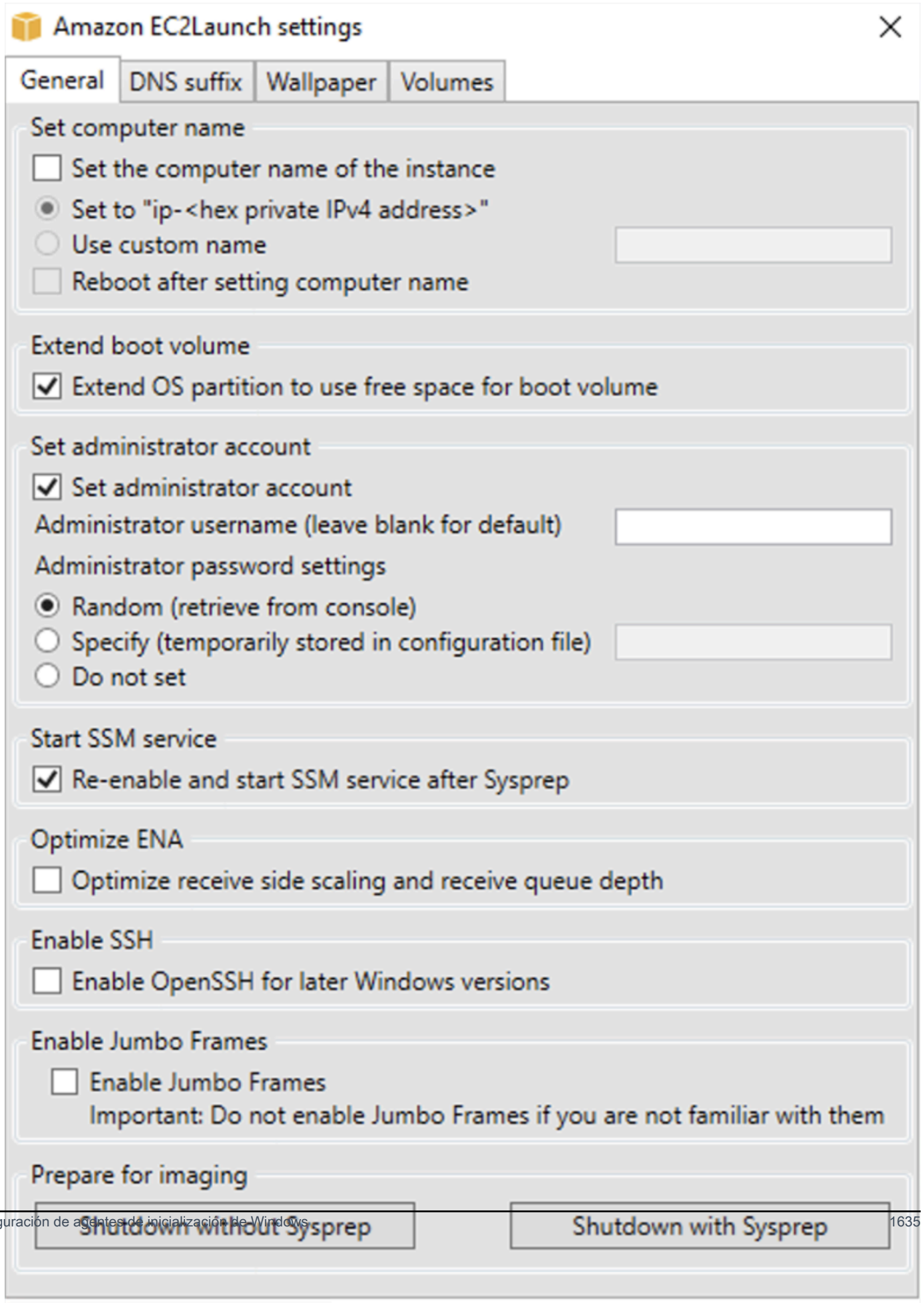
- Cambiar la configuración mediante el cuadro de diálogo de configuración de EC2Launch v2
- Estructura del directorio de EC2Launch v2
- Configurar EC2Launch v2 mediante la CLI
- Configuración de tareas de EC2Launch v2
- Códigos de salida y reinicios de EC2Launch v2
- EC2Launch v2 y Sysprep

Cambiar la configuración mediante el cuadro de diálogo de configuración de EC2Launch v2

El siguiente procedimiento describe cómo utilizar el cuadro de diálogo de configuración de EC2Launch v2 para habilitar o desactivar la configuración.

> **Note**
>
> Si configuró de forma incorrecta las tareas personalizadas en el archivo agent-config.yml e intenta abrir el cuadro de diálogo configuración de Amazon EC2Launch, recibirá un mensaje de error. Para ver un esquema de ejemplo, consulte Ejemplo: `agent-config.yml`.

1. Lance y conéctese a la instancia de Windows.
2. En el menú Inicio, elija Todos los programas y, a continuación, vaya a la Configuración de EC2Launch.


Amazon EC2Launch settings
General
DNS suffix
Wallpaper
Volumes
Set computer name
Set the computer name of the instance
Set to "ip-<hex private IPv4 address>"
Use custom name
Reboot after setting computer name
Extend boot volume
Extend OS partition to use free space for boot volume
Set administrator account
Set administrator account
Administrator username (leave blank for default)
Administrator password settings
Random (retrieve from console)
Specify (temporarily stored in configuration file)
Do not set
Start SSM service
Re-enable and start SSM service after Sysprep
Optimize ENA
Optimize receive side scaling and receive queue depth
Enable SSH
Enable OpenSSH for later Windows versions
Enable Jumbo Frames
Enable Jumbo Frames
Important: Do not enable Jumbo Frames if you are not familiar with them
Prepare for imaging
Shutdown without Sysprep
Shutdown with Sysprep

3. En la pestaña General del cuadro de diálogo Configuración de EC2Launch, puede habilitar o desactivar la siguiente configuración.

   a. Set Computer Name (Establecer nombre del equipo)

      Si esta configuración está habilitada (está desactivada de forma predeterminada), el nombre de host actual se compara con el nombre de host deseado en cada arranque. Si los nombres de host no coinciden, el nombre de host se restablece y el sistema, opcionalmente, se reinicia para recoger el nuevo nombre de host. Si no se especifica un nombre de host personalizado, se genera mediante la dirección IPv4 privada con formato hexadecimal, por ejemplo, `ip-AC1F4E6`. Para evitar que se modifique el nombre de host no habilite esta opción.

   b. Extender volumen de arranque

      Esta opción amplía dinámicamente `Disk 0`/`Volume 0` para incluir cualquier espacio sin particionar. Esto puede resultar útil cuando la instancia se arranca desde un volumen de dispositivo raíz con un tamaño personalizado.

   c. Establecer cuenta de administrador

      Cuando está habilitado, puede establecer los atributos de nombre de usuario y contraseña para la cuenta de administrador que se crea en el equipo local. Si esta característica no está habilitada, no se crea una cuenta de administrador en el sistema después de Sysprep. Proporcione una contraseña en `adminPassword` solo si `adminPasswordtype` es `Specify`.

      Los tipos de contraseñas se definen de la siguiente manera:

      i. `Random`

         EC2Launch genera una contraseña y la cifra usando la clave del usuario. El sistema deshabilita esta configuración tras la inicialización de la instancia para que esta contraseña persista si la instancia se reinicia o si se detiene y se inicia.

      ii. `Specify`

         EC2Launch usa la contraseña que ha especificado en `adminPassword`. Si la contraseña no cumple los requisitos del sistema, EC2Launch genera una contraseña aleatoria en su lugar. La contraseña se almacena en `agent-config.yml` como

texto sin cifrar y se elimina cuando Sysprep define la contraseña del administrador. EC2Launch cifra la contraseña usando la clave del usuario.

iii. `Do not set`

EC2Launch utiliza la contraseña especificada en el archivo unattend.xml. Si no especifica una contraseña en unattend.xml, la cuenta del administrador se desactiva.

d. Iniciar servicio SSM

Cuando se selecciona, el servicio Systems Manager queda habilitado para comenzar después de Sysprep. EC2Launch v2 realiza todas las tareas descritas anteriormente, y SSM Agent procesa las solicitudes para las funcionalidades de Systems Manager, como Run Command y administrador de estados.

Puede usar Run Command para actualizar las instancias existentes de manera que utilicen la versión más reciente del servicio EC2Launch v2 y de SSM Agent. Para obtener más información, consulte Actualizar SSM Agent utilizando Run Command en la Guía del usuario de Systems Manager de AWS.

e. Optimizar ENA

Cuando se selecciona, la configuración de ENA se configura para garantizar que la configuración del escalado del lado de recepción de ENA y la configuración de profundidad de cola de recepción se optimizan para AWS. Para obtener más información, consulte Configurar la afinidad de la CPU de RSS.

f. Habilitar SSH

Esta configuración habilita OpenSSH para versiones posteriores de Windows para permitir la administración remota del sistema.

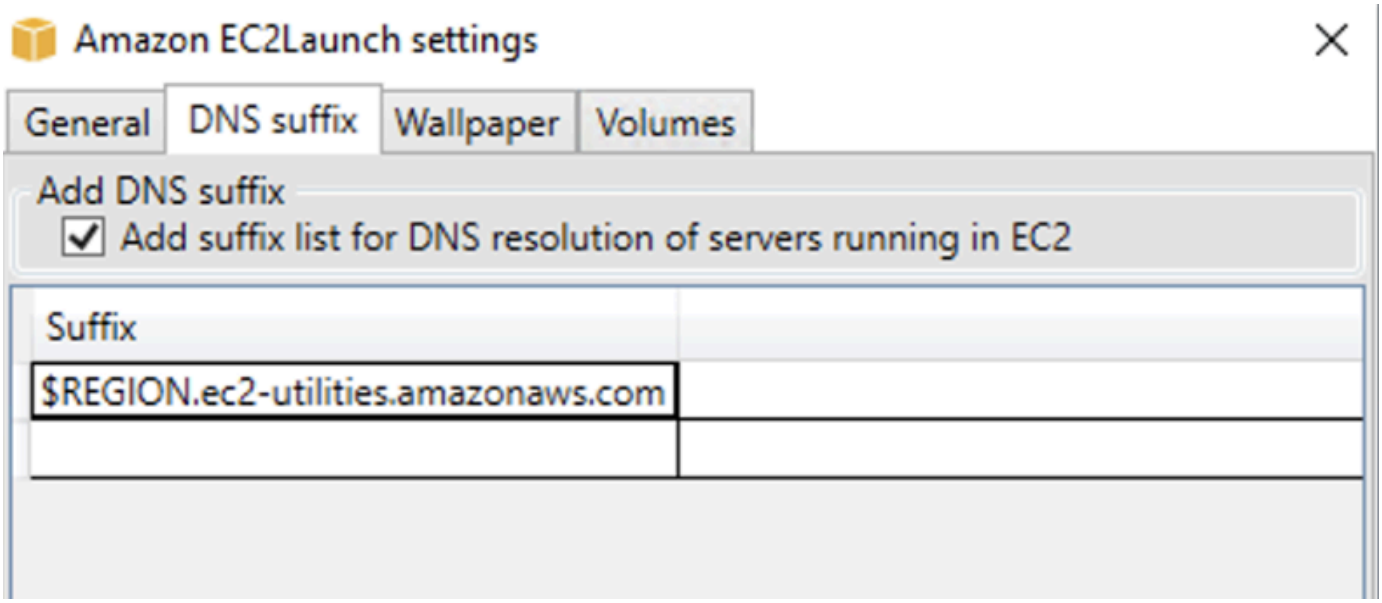
g. Habilitar tramas gigantes

Seleccione esta opción para habilitar las tramas gigantes. Las tramas gigantes pueden tener efectos no deseados en las comunicaciones de red, así que asegúrese de comprender cómo afectarán las tramas gigantes al sistema antes de habilitarlas. Para obtener más información acerca de las tramas gigantes, consulte Tramas gigantes (9 001 MTU).

h. Preparativos para la creación de imágenes

Seleccione si desea que su instancia de EC2 se cierre con o sin Sysprep. Cuando desee ejecutar Sysprep con EC2Launch v2, elija “Shutdown with Sysprep” (Apagar con Sysprep).

4. En la pestaña Sufijo de DNS, puede seleccionar si desea agregar una lista de sufijos DNS para la resolución DNS de los servidores que se ejecutan en EC2, sin proporcionar el nombre de dominio completo. Los sufijos de DNS pueden contener las variables `$REGION` y `$AZ`. Solo se agregarán a la lista los sufijos que aún no existan.



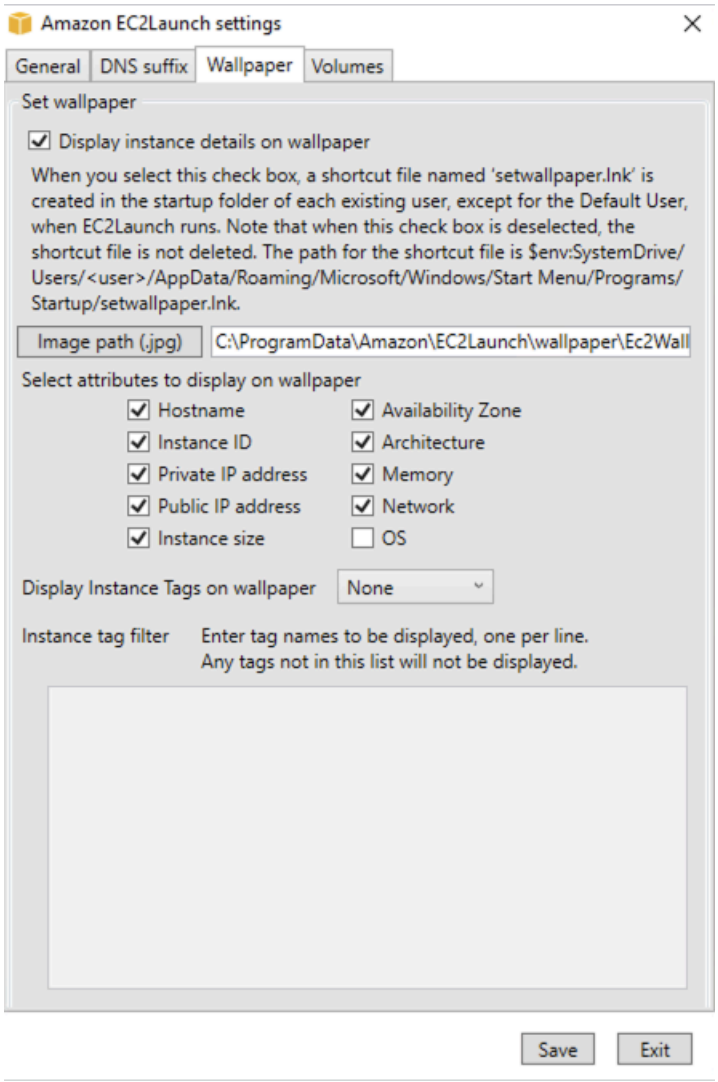
5. En la pestaña Fondo de pantalla, puede configurar el fondo de pantalla de la instancia con una imagen de fondo y especificar los detalles de la instancia para que se muestre el fondo de pantalla. Amazon EC2 genera los detalles cada vez que inicia sesión.

   Puede configurar su fondo de pantalla con los siguientes controles.

   - Mostrar detalles de la instancia en el fondo de pantalla: esta casilla de verificación activa o desactiva la visualización de detalles de la instancia en el fondo de pantalla.
   - Ruta de la imagen (.jpg): especifique la ruta a la imagen que se va a utilizar como fondo de pantalla.
   - Seleccionar atributos que mostrar en el fondo de pantalla: seleccione las casillas con los detalles de la instancia que quiere que aparezcan en el fondo de pantalla. Desactive las casillas de verificación que anteriormente seleccionadas para detalles de instancias que quiere eliminar del fondo de pantalla.
   - Mostrar etiquetas de la instancia en el fondo de pantalla: seleccione una de las siguientes configuraciones para mostrar etiquetas de la instancia en el fondo de pantalla:
     - Ninguna: no muestra ninguna etiqueta de instancia en el fondo de pantalla.
     - Mostrar todas: muestra todas las etiquetas de instancia en el fondo de pantalla.

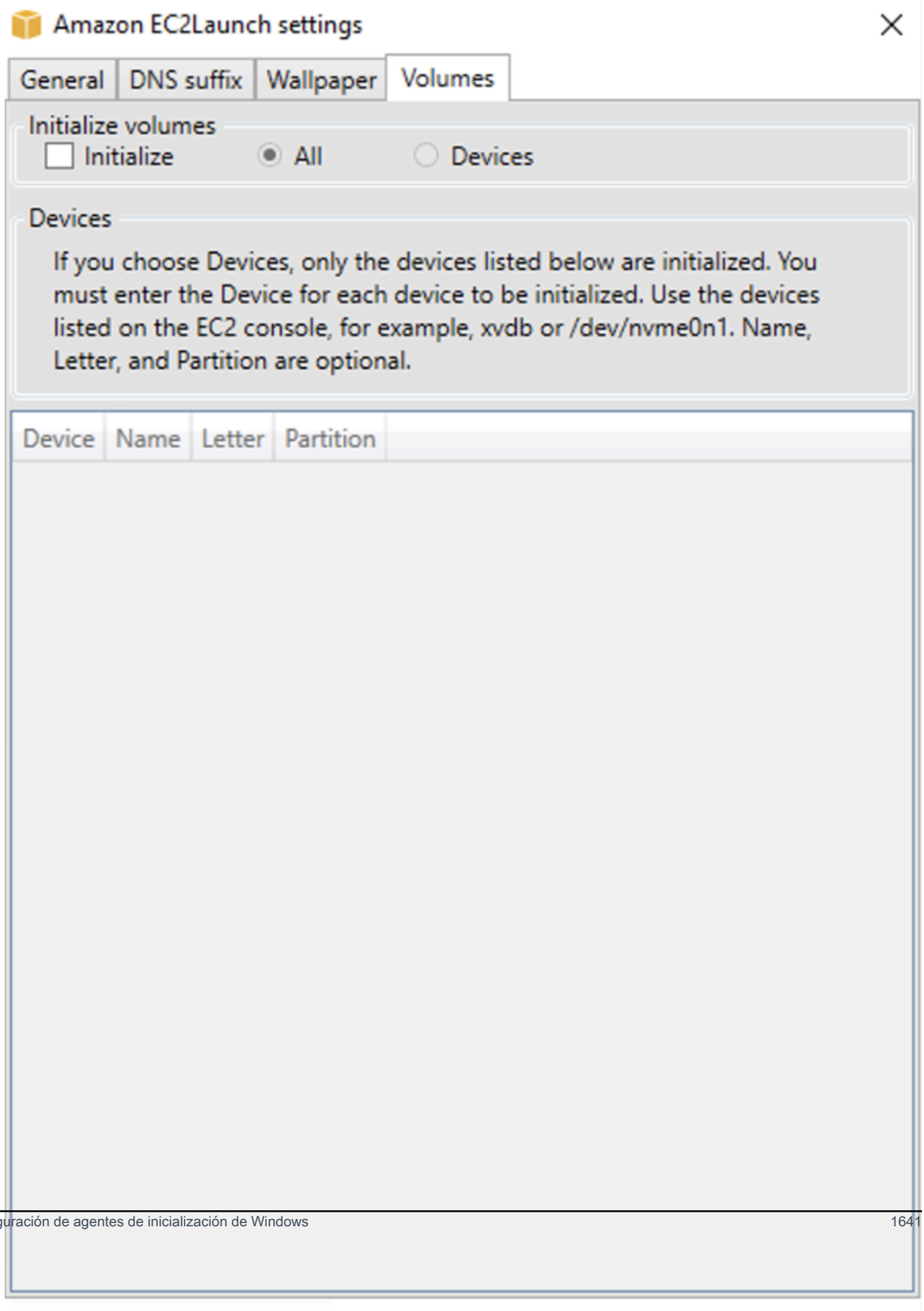
- Mostrar solo las filtradas: muestra las etiquetas de instancia especificadas en el fondo de pantalla. Al seleccionar esta configuración, puede agregar las etiquetas de instancia que quiera que se muestren en su fondo de pantalla en el cuadro Filtro de etiquetas de instancia.

> **Note**
>
> Debe habilitar las etiquetas en los metadatos para que se muestren en el fondo de pantalla. Para obtener más información acerca de las etiquetas y metadatos de instancias, consulte Trabajar con etiquetas de instancia en los metadatos de instancia.



6. En la pestaña Volúmenes, seleccione si desea inicializar los volúmenes asociados a la instancia. La habilitación establece letras de unidad para cualquier volumen adicional y las amplía para utilizar el espacio disponible. Si selecciona Todo, se inicializarán todos los volúmenes de almacenamiento. Si selecciona Dispositivos, solo se inicializarán los dispositivos especificados en la lista. Debe escribir el dispositivo para cada dispositivo que se inicialice. Utilice los dispositivos enumerados en la consola de EC2, por ejemplo, `xvdb` o `/dev/nvme0n1`. La lista desplegable muestra los volúmenes de almacenamiento asociados a la instancia. Para introducir un dispositivo que no esté asociado a la instancia, escríbalo en el campo de texto.

   Nombre, Letra y Partición son campos opcionales. Si no se especifica ningún valor para Partición, los volúmenes de almacenamiento más grandes que 2 TB se inicializan con el tipo de partición `gpt`, mientras que los más chicos que 2 TB se inicializan con el tipo de partición `mbr`. Si los dispositivos están configurados y un dispositivo que no sea NTFS contiene una tabla de particiones o los primeros 4 KB del disco contienen datos, se omite el disco y se registra la acción.


Amazon EC2Launch settings
General
DNS suffix
Wallpaper
Volumes
Initialize volumes
Initialize
All
Devices
Devices
If you choose Devices, only the devices listed below are initialized. You must enter the Device for each device to be initialized. Use the devices listed on the EC2 console, for example, xvdb or /dev/nvme0n1. Name, Letter, and Partition are optional.
Device
Name
Letter
Partition

A continuación se muestra un archivo YAML de configuración de ejemplo creado a partir de los parámetros escritos en el cuadro de diálogo EC2Launch.

```
version: 1.0
config:
  - stage: boot
 tasks:
      - task: extendRootPartition
  - stage: preReady
    tasks:
      - task: activateWindows
        inputs:
          activation:
            type: amazon
      - task: setDnsSuffix
        inputs:
          suffixes:
            - $REGION.ec2-utilities.amazonaws.com
      - task: setAdminAccount
        inputs:
          password:
            type: random
      - task: setWallpaper
        inputs:
          path: C:\ProgramData\Amazon\EC2Launch\wallpaper\Ec2Wallpaper.jpg
          attributes:
            - hostName
            - instanceId
            - privateIpAddress
            - publicIpAddress
            - instanceSize
            - availabilityZone
            - architecture
            - memory
            - network
  - stage: postReady
    tasks:
      - task: startSsm
```

Estructura del directorio de EC2Launch v2

EC2Launch v2 debe instalarse en los siguientes directorios:

- Binarios de servicio: `%ProgramFiles%\Amazon\EC2Launch`
- Datos del servicio (configuración, archivos de registro y archivos de estado): `%ProgramData%\Amazon\EC2Launch`

> **Note**
>
> De manera predeterminada, Windows oculta los archivos y las carpetas en `C:\ProgramData`. Para ver los directorios y los archivos de EC2Launch v2, debe ingresar la ruta en Windows Explorer o cambiar las propiedades de la carpeta para mostrar los archivos y las carpetas ocultos.

El directorio `%ProgramFiles%\Amazon\EC2Launch` contiene binarios y bibliotecas auxiliares. Incluye los siguientes subdirectorios:

- `settings`
  - `EC2LaunchSettingsUI.exe`: interfaz de usuario para modificar el archivo `agent-config.yml`
  - `YamlDotNet.dll`: DLL para admitir algunas operaciones en la interfaz de usuario
- `tools`
  - `ebsnvme-id.exe`: herramienta para examinar los metadatos de los volúmenes de EBS en la instancia
  - `AWSAcpiSpcrReader.exe`: herramienta para determinar el puerto COM correcto a usar
  - `EC2LaunchEventMessage.dll`: DLL para admitir el registro de eventos de Windows para EC2Launch.
- `service`
  - `EC2LaunchService.exe` — Ejecutable de servicio de Windows que se inicia cuando el agente de inicialización se ejecuta como un servicio.
- `EC2Launch.exe`: ejecutable principal de EC2Launch
- `EC2LaunchAgentAttribution.txt`: atribución del código utilizado en EC2 Launch

El directorio `%ProgramData%\Amazon\EC2Launch` contiene los subdirectorios siguientes. Todos los datos producidos por el servicio, incluidos los registros, la configuración y el estado, se almacenan en este directorio.

- `config`: configuración

  El archivo de configuración del servicio se almacena en este directorio como `agent-config.yml`. Este archivo se puede actualizar para modificar, agregar o eliminar tareas predeterminadas ejecutadas por el servicio. El permiso para crear archivos en este directorio se encuentra restringido a la cuenta de administrador a fin de evitar la escalada de privilegios.

- `log`: registros de instancias

  Los registros del servicio (`agent.log`), la consola (`console.log`), el rendimiento (`bench.log`) y los errores (`error.log`) se almacenan en este directorio. Los archivos de registro se anexan en las ejecuciones posteriores del servicio.

- `state`: datos del estado del servicio

  El estado que utiliza el servicio para determinar qué tareas deben ejecutarse se almacena aquí. Hay un archivo `.run-once` que indica si el servicio ya se ejecutó después de Sysprep (por lo que las tareas con una frecuencia de una vez se omitirán en la siguiente ejecución). Este subdirectorio incluye un `state.json` y `previous-state.json` para realizar un seguimiento del estado de cada tarea.

- `sysprep`: Sysprep

  Este directorio contiene archivos que se utilizan para determinar qué operaciones debe realizar Sysprep cuando crea una AMI de Windows personalizada que se puede reutilizar.

Configurar EC2Launch v2 mediante la CLI

Puede utilizar la interfaz de línea de comandos (CLI) para ajustar la configuración de EC2Launch y administrar el servicio. La siguiente sección contiene descripciones e información de uso de los comandos de la CLI que puede utilizar para administrar EC2Launch v2.

Comandos

- collect-logs
- get-agent-config
- list-volumes
- reset
- run
- estado

- sysprep
- validar
- versión
- fondo de pantalla

collect-logs

Recopila archivos de registro para EC2Launch, comprime los archivos y los coloca en un directorio especificado.

Ejemplo

```
ec2launch collect-logs -o C:\Mylogs.zip
```

Uso

`ec2launch collect-logs [flags]`

Flags

`-h, --help`

ayuda para `collect-logs`

`-o, --output string`

ruta a los archivos de registro de salida comprimidos

get-agent-config

Imprime `agent-config.yml` en el formato especificado (JSON o YAML). Si no se especifica ningún formato, `agent-config.yml` se imprime en el formato especificado anteriormente.

Ejemplo

```
ec2launch get-agent-config -f json
```

Ejemplo 2

Los siguientes comandos de PowerShell muestran cómo editar y guardar el archivo `agent-config` en formato JSON.

```
$config = & "$env:ProgramFiles/Amazon/EC2Launch/EC2Launch.exe" --format json |
 ConvertFrom-Json
$jumboFrame =@"
{
   "task": "enableJumboFrames"
}
"@
$config.config | %{if($_.stage -eq 'postReady'){$_.tasks += (ConvertFrom-Json -
InputObject $jumboFrame)}}
$config | ConvertTo-Json -Depth 6 | Out-File -encoding UTF8
$env:ProgramData/Amazon/EC2Launch/config/agent-config.yml
```

Uso

`ec2launch get-agent-config [flags]`

Flags

`-h`, `--help`

ayuda para `get-agent-config`

`-f`, `--format string`

formato de salida del archivo `agent-config`: `json`, `yaml`

list-volumes

Muestra todos los volúmenes de almacenamiento asociados a la instancia, incluidos los volúmenes efímeros y de EBS.

Ejemplo

```
ec2launch list-volumes
```

Uso

`ec2launch list-volumes`

Flags

`-h`, `--help`

ayuda para `list-volumes`

reset

El objetivo principal de esta tarea es restablecer el agente para la próxima vez que se ejecute. Con este objetivo, el comando reset elimina todos los datos de estado del agente para EC2Launch v2 del directorio local de `EC2Launch` (consulte Estructura del directorio de EC2Launch v2). Restablecer elimina de manera opcional el servicio y los registros de Sysprep.

El comportamiento de los scripts depende del modo en el que el agente los ejecute: en línea o de forma independiente.

En línea (predeterminado)

El agente de EC2Launch v2 ejecuta los scripts de uno en uno (`detach: false`). Este es el valor predeterminado.

> **Note**
>
> Cuando el script en línea emite un comando reset o sysprep, se ejecuta de manera inmediata y restablece el agente. La tarea actual finaliza y, a continuación, el agente se cierra sin ejecutar ninguna otra tarea.
> Por ejemplo, si la tarea que emite el comando hubiera estado seguida de una tarea `startSsm` (incluida de forma predeterminada cuando se ejecutan los datos del usuario), la tarea no se ejecutaría y el servicio Systems Manager nunca se iniciaría.

Desconectado

El agente EC2Launch v2 ejecuta scripts de manera simultánea a otras tareas (`detach: true`).

> **Note**
>
> Cuando el script independiente emite un comando reset o sysprep, dichos comandos esperan a que el agente termine antes de ejecutarse. Las tareas posteriores a executeScript seguirán ejecutándose.

Ejemplo

```
ec2launch reset -c
```

Uso

`ec2launch reset [flags]`

Flags

`-c`, `--clean`

limpia los registros de instancias antes de `reset`

`-h`, `--help`

ayuda para `reset`

run

Ejecuciones de EC2Launch v2.

Ejemplo

```
ec2launch run
```

Uso

`ec2launch run [flags]`

Flags

`-h`, `--help`

ayuda para `run`

estado

Obtiene el estado del agente EC2Launch v2. Opcionalmente bloquea el proceso hasta que finalice el agente. El código de salida del proceso determina el estado del agente:

- `0`: el agente se ejecutó con éxito.
- `1`: el agente se ejecutó de forma incorrecta.
- `2`: el agente sigue en ejecución.
- `3`: el agente se encuentra en estado desconocido. El estado del agente es detenido o sin ejecución.

- 4: se produjo un error al intentar recuperar el estado del agente.
- 5: el agente no se está ejecutando y se desconoce el estado de la última ejecución registrada. Esto podría significar una de las siguientes opciones:
  - tanto el `state.json` y `previous-state.json` se han eliminado.
  - el `previous-state.json` se encuentra dañado.

  Este es el estado del agente después de ejecutar el comando `reset`.

Ejemplo:

```
ec2launch status -b
```

Uso

`ec2launch status [flags]`

Flags

`-b,--block`

bloquea el proceso hasta que el agente termine de ejecutarse

`-h,--help`

ayuda para `status`

sysprep

El objetivo principal de esta tarea es restablecer el agente para la próxima vez que se ejecute. Para ello, el comando sysprep restablece el estado del agente, actualiza el archivo `unattend.xml`, desactiva RDP y ejecuta Sysprep.

El comportamiento de los scripts depende del modo en el que el agente los ejecute: en línea o de forma independiente.

En línea (predeterminado)

El agente de EC2Launch v2 ejecuta los scripts de uno en uno (`detach: false`). Este es el valor predeterminado.

> **Note**
>
> Cuando el script en línea emite un comando reset o sysprep, se ejecuta de manera inmediata y restablece el agente. La tarea actual finaliza y, a continuación, el agente se cierra sin ejecutar ninguna otra tarea.
> Por ejemplo, si la tarea que emite el comando hubiera estado seguida de una tarea `startSsm` (incluida de forma predeterminada cuando se ejecutan los datos del usuario), la tarea no se ejecutaría y el servicio Systems Manager nunca se iniciaría.

Desconectado

El agente EC2Launch v2 ejecuta scripts de manera simultánea a otras tareas (`detach: true`).

> **Note**
>
> Cuando el script independiente emite un comando reset o sysprep, dichos comandos esperan a que el agente termine antes de ejecutarse. Las tareas posteriores a executeScript seguirán ejecutándose.

Ejemplo:

```
ec2launch sysprep
```

Uso

`ec2launch sysprep [flags]`

Flags

`-c,--clean`

limpia los registros de instancias antes de `sysprep`

`-h,--help`

ayuda para Sysprep

`-s,--shutdown`

cierra la instancia después de `sysprep`

validar

Valida el archivo `agent-config` `C:\ProgramData\Amazon\EC2Launch\config\agent-config.yml`.

Ejemplo

```
ec2launch validate
```

Uso

`ec2launch validate [flags]`

Flags

`-h` , `--help`

ayuda para `validate`

versión

Obtiene la versión ejecutable.

Ejemplo

```
ec2launch version
```

Uso

`ec2launch version [flags]`

Flags

`-h`, `--help`

ayuda para `version`

fondo de pantalla

Establece el nuevo fondo de pantalla en la ruta de fondo de pantalla que se proporciona (archivo .jpg) y muestra los detalles de la instancia seleccionada.

Sintaxis

```
ec2launch wallpaper ^
--path="C:\ProgramData\Amazon\EC2Launch\wallpaper\Ec2Wallpaper.jpg" ^
--all-tags ^
--
attributes=hostName,instanceId,privateIpAddress,publicIpAddress,instanceSize,availabilityZone,a
```

Entradas

Parámetros

--allowed-tags [*`nombre-etiqueta-1`*, *`nombre-etiqueta-n`*]

(Opcional) Matriz JSON codificada en Base64 de nombres de etiquetas de instancia para mostrarla en el fondo de pantalla. Puede utilizar esta etiqueta o `--all-tags`, pero no ambas.

--attributes *`cadena-de-atributos-1`*, *`cadena-de-atributos-n`*

(Opcional) Lista separada por comas de `wallpaper` cadenas de atributos para aplicar la configuración al fondo de pantalla.

[--path| -p] *`cadena-de-ruta`*

(Obligatorio) Especifique la ruta del archivo de imagen de fondo de `wallpaper`.

Indicadores

--all-tags

(Opcional) Muestre todas las etiquetas de instancia en el fondo de pantalla. Puede utilizar esta etiqueta o `--allowed-tags`, pero no ambas.

[--help | -h]

Muestra ayuda para el comando wallpaper.

Configuración de tareas de EC2Launch v2

Esta sección incluye el esquema de configuración, las tareas, detalles y ejemplos para `agent-config.yml` y datos del usuario.

Tareas y ejemplos

- Esquema: agent-config.yml
- Esquema: datos de usuario
- Definiciones de tareas

Esquema: **`agent-config.yml`**

La estructura del archivo `agent-config.yml` se muestra a continuación. Tenga en cuenta que no es posible repetir una tarea en la misma etapa. Para ver las propiedades de las tareas, consulte las descripciones de tareas siguientes.

Estructura del documento: agent-config.yml

JSON

```
{
 "version": "1.0",
 "config": [
  {
   "stage": "string",
   "tasks": [
    {
     "task": "string",
     "inputs": {
      ...
     }
    },
    ...
   ]
  },
  ...
 ]
}
```

YAML

```
version: 1.0
config:
- stage: string
  tasks:
  - task: string
 inputs:
```

```
   ...
  ...
...
```

Ejemplo: **`agent-config.yml`**

En el ejemplo siguiente se muestran los valores del archivo de configuración `agent-config.yml`.

```
version: 1.0
config:
- stage: boot
  tasks:
  - task: extendRootPartition
- stage: preReady
  tasks:
  - task: activateWindows
    inputs:
      activation:
        type: amazon
  - task: setDnsSuffix
    inputs:
      suffixes:
      - $REGION.ec2-utilities.amazonaws.com
  - task: setAdminAccount
    inputs:
      password:
        type: random
  - task: setWallpaper
    inputs:
      path: C:\ProgramData\Amazon\EC2Launch\wallpaper\Ec2Wallpaper.jpg
      attributes:
      - hostName
      - instanceId
      - privateIpAddress
      - publicIpAddress
      - instanceSize
      - availabilityZone
      - architecture
      - memory
      - network
- stage: postReady
  tasks:
  - task: startSsm
```

Esquema: datos de usuario

Los siguientes ejemplos de JSON y YAML muestran la estructura del documento para los datos de usuario. Amazon EC2 analiza cada tarea nombrada en la matriz `tasks` que especifique en el documento. Cada tarea tiene su propio conjunto de propiedades y requisitos. Para obtener información detallada, consulte Definiciones de tareas.

> **Note**
>
> Una tarea solo debe aparecer una vez en la matriz de tareas de datos de usuario.

Estructura del documento: datos de usuario

JSON

```
{
 "version": "1.1",
 "tasks": [
  {
   "task": "string",
   "inputs": {
    ...
   },
  },
  ...
 ]
}
```

YAML

```
version: 1.1
tasks:
- task: string
  inputs:
    ...
...
```

Ejemplo: datos de usuario

Para obtener más información sobre datos de usuario, consulte Cómo gestiona Amazon EC2 los datos de usuario de las instancias de Windows.

El siguiente ejemplo de documento YAML muestra un script de PowerShell que EC2Launch v2 ejecuta como datos de usuario para crear un archivo.

```
version: 1.1
tasks:
- task: executeScript
  inputs:
  - frequency: always
    type: powershell
    runAs: localSystem
    content: |-
      New-Item -Path 'C:\PowerShellTest.txt' -ItemType File
```

Puede utilizar un formato XML para los datos de usuario que sea compatible con las versiones anteriores del agente de inicialización. EC2Launch v2 ejecuta el script como una tarea `executeScript` en la etapa `UserData`. Para cumplir con el comportamiento de EC2Launch v1 y EC2Config, el script de datos del usuario se ejecuta como un proceso adjunto o en línea de forma predeterminada.

Puede agregar etiquetas opcionales para personalizar la ejecución del script. Por ejemplo, para ejecutar el script de datos de usuario cuando la instancia se reinicia, además de ejecutarse una vez cuando se inicia la instancia, puede usar la siguiente etiqueta:

`<persist>true</persist>`

Ejemplo:

```
<powershell>
  $file = $env:SystemRoot + "\Temp" + (Get-Date).ToString("MM-dd-yy-hh-mm")
  New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

Puede especificar uno o varios argumentos de PowerShell con la etiqueta `<powershellArguments>`. Si no se pasa ningún argumento, EC2Launch v2 agrega el siguiente argumento de forma predeterminada: `-ExecutionPolicy Unrestricted`.

Ejemplo:

```
<powershell>
  $file = $env:SystemRoot + "\Temp" + (Get-Date).ToString("MM-dd-yy-hh-mm")
```

```
  New-Item $file -ItemType file
</powershell>
<powershellArguments>-ExecutionPolicy Unrestricted -NoProfile -NonInteractive</
powershellArguments>
```

Para ejecutar un script de datos de usuario XML como un proceso independiente, agregue la siguiente etiqueta a sus datos de usuario.

```
<detach>true</detach>
```

Ejemplo:

```
<powershell>
  $file = $env:SystemRoot + "\Temp" + (Get-Date).ToString("MM-dd-yy-hh-mm")
  New-Item $file -ItemType file
</powershell>
<detach>true</detach>
```

> **Note**
>
> La etiqueta de desconexión no es compatible con los agentes de inicialización anteriores.

Registro de cambios: datos de usuario

La siguiente tabla muestra los cambios en los datos de usuario y los compara con la versión del agente EC2Launch v2 aplicable.

Versión de datos de usuario	Detalles	Presentación
1.1	• Las tareas de datos de usuario se ejecutan antes de la etapa `PostReady` en el archivo de configuración del agente. • Ejecuta datos de usuario antes de iniciar Systems Manager Agent (el mismo comportamiento que EC2Launch v1 y EC2Config).*	EC2Launch v2, versión 2.0.1245

Versión de datos de usuario	Detalles	Presentación
1.0	• Quedará en desuso. • Las tareas de datos de usuario se ejecutan después de la etapa `PostReady` en el archivo de configuración del agente. Esto no es compatible con versiones anteriores de EC2Launch v1. • Se ve afectado por una situación de carrera entre el inicio de Systems Manager Agent y las tareas de datos del usuario.	EC2Launch v2, versión 2.0.0

* Cuando se usa con el archivo `agent-config.yml` predeterminado.

Definiciones de tareas

Cada tarea tiene su propio conjunto de propiedades y requisitos. Para obtener información detallada, consulte las tareas individuales que desee incluir en el documento.

Tareas

- activateWindows
- enableJumboFrames
- enableOpenSsh
- executeProgram
- executeScript
- extendRootPartition
- initializeVolume
- optimizeEna
- setAdminAccount
- setDnsSuffix
- setHostName
- setWallpaper

- startSsm
- sysprep
- writeFile

activateWindows

Activa Windows frente a un conjunto de servidores AWS KMS. La activación se omite si se detecta que la instancia es de tipo “traiga su propia licencia (BYOL)”.

Frecuencia: una vez

AllowedStages — `[PreReady]`

Entradas —

`activation`: (mapa)

`type`: (cadena) tipo de activación que se va a utilizar, se establece en `amazon`

Ejemplo

```
task: activateWindows
inputs:
  activation:
    type: amazon
```

enableJumboFrames

Habilita tramas gigantes, que aumentan la unidad de transmisión máxima (MTU) del adaptador de red. Para obtener más información, consulte Tramas gigantes (9 001 MTU).

Frecuencia: siempre

AllowedStages — `[PostReady, UserData]`

Entradas: ninguna

Ejemplo

```
task: enableJumboFrames
```

enableOpenSsh

Habilita Windows OpenSSH y agrega la clave pública de la instancia a la carpeta de claves autorizadas.

Frecuencia: una vez

AllowedStages — `[PreReady, UserData]`

Entradas: ninguna

Ejemplo

En el ejemplo siguiente se muestra cómo habilitar OpenSSH en una instancia y agregar la clave pública de la instancia a la carpeta de claves autorizadas. Esta configuración solo funciona en instancias que ejecutan Windows Server 2019 y en versiones posteriores.

```
task: enableOpenSsh
```

executeProgram

Ejecuta un programa con argumentos opcionales y una frecuencia especificada.

Etapas: puede ejecutar la tarea `executeProgram` durante las etapas `PreReady`, `PostReady` y `UserData`.

Frecuencia: configurable, consulte Entradas.

Entradas

Puede configurar los parámetros de tiempo de ejecución de la siguiente manera:

frequency (cadena)

(Obligatorio) Especifique exactamente uno de los siguientes valores:

- `once`
- `always`

ruta (cadena)

(Obligatorio) La ruta del archivo para el ejecutable a ejecutar.

arguments (lista de cadenas)

(Opcional) Una lista de argumentos separados por comas para proporcionar al programa como entrada.

runAs (cadena)

(Obligatorio) Debe configurarse en `localSystem`

Salida

Todas las tareas escriben las entradas del archivo de registro en el archivo `agent.log`. Los resultados adicionales de la tarea `executeProgram` se almacenan por separado en una carpeta con nombre dinámico, de la siguiente manera:

`%LocalAppData%\Temp\`*`EC2Launch#########`*`\`*`outputfilename.tmp`*

La ruta exacta a los archivos de salida se incluye en el archivo `agent.log`, por ejemplo:

```
Program file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\ExecuteProgramInputs.tmp
Output file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\Output.tmp
Error file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\Err.tmp
```

Archivos de salida para la tarea **`executeProgram`**

`ExecuteProgramInputs.tmp`

Contiene la ruta del ejecutable y todos los parámetros de entrada que la tarea `executeProgram` le transfiere cuando se ejecuta.

`Output.tmp`

Contiene la salida del tiempo de ejecución del programa en el que se ejecuta la tarea `executeProgram`.

`Err.tmp`

Contiene el error del tiempo de ejecución del programa en el que se ejecuta la tarea `executeProgram`.

Ejemplos

En los siguientes ejemplos, se muestra cómo ejecutar un archivo ejecutable desde un directorio local en una instancia con la tarea `executeProgram`.

Ejemplo 1: Configurar el ejecutable con un argumento

En este ejemplo, se muestra una tarea `executeProgram` que ejecuta un ejecutable de configuración en modo silencioso.

```
task: executeProgram
inputs:
- frequency: always
  path: C:\Users\Administrator\Desktop\setup.exe
  arguments: ['-quiet']
```

Ejemplo 2: Ejecutable de VLC con dos argumentos

Este ejemplo muestra una tarea `executeProgram` que ejecuta un archivo ejecutable de VLC con dos argumentos pasados como parámetros de entrada.

```
task: executeProgram
inputs:
- frequency: always
  path: C:\vlc-3.0.11-win64.exe
  arguments: ['/L=1033','/S']
  runAs: localSystem
```

executeScript

Ejecuta un script con argumentos opcionales y una frecuencia especificada. El comportamiento de los scripts depende del modo en el que el agente los ejecute: en línea o de forma independiente.

En línea (predeterminado)

El agente de EC2Launch v2 ejecuta los scripts de uno en uno (`detach: false`). Este es el valor predeterminado.

> **Note**
>
> Cuando el script en línea emite un comando reset o sysprep, se ejecuta de manera inmediata y restablece el agente. La tarea actual finaliza y, a continuación, el agente se cierra sin ejecutar ninguna otra tarea.
> Por ejemplo, si la tarea que emite el comando hubiera estado seguida de una tarea `startSsm` (incluida de forma predeterminada cuando se ejecutan los datos del usuario), la tarea no se ejecutaría y el servicio Systems Manager nunca se iniciaría.

Desconectado

El agente EC2Launch v2 ejecuta scripts de manera simultánea a otras tareas (`detach: true`).

> **Note**
>
> Cuando el script independiente emite un comando reset o sysprep, dichos comandos esperan a que el agente termine antes de ejecutarse. Las tareas posteriores a executeScript seguirán ejecutándose.

Etapas: puede ejecutar la tarea `executeScript` durante las etapas `PreReady`, `PostReady` y `UserData`.

Frecuencia: configurable, consulte Entradas.

Entradas

Puede configurar los parámetros de tiempo de ejecución de la siguiente manera:

frequency (cadena)

(Obligatorio) Especifique exactamente uno de los siguientes valores:

- `once`
- `always`

type (cadena)

(Obligatorio) Especifique exactamente uno de los siguientes valores:

- `batch`

- `powershell`

arguments (lista de cadenas)

(Opcional) Una lista de argumentos de cadena para pasar al shell. Este parámetro no es compatible con `type: batch`. Si no se pasa ningún argumento, EC2Launch v2 agrega el siguiente argumento de forma predeterminada: `-ExecutionPolicy Unrestricted`.

content (cadena)

(Obligatorio) Contenido de script.

runAs (cadena)

(Obligatorio) Especifique exactamente uno de los siguientes valores:

- `admin`
- `localSystem`

detach (booleano)

(Opcional) El agente EC2Launch v2 ejecuta de forma predeterminada los scripts de uno en uno (`detach: false`). Para ejecutar el script simultáneamente con otras tareas, defina el valor en `true` (`detach: true`).

> **Note**
>
> Los códigos de salida de script (incluido `3010`) no surten efecto cuando `detach` está establecido como `true`.

Salida

Todas las tareas escriben las entradas del archivo de registro en el archivo `agent.log`. La salida adicional del script que ejecuta la tarea `executeScript` se almacena por separado en una carpeta con nombre dinámico, de la siguiente manera:

`%LocalAppData%\Temp\`*`EC2Launch#########`*`\`*`outputfilename.ext`*

La ruta exacta a los archivos de salida se incluye en el archivo `agent.log`, por ejemplo:

```
Program file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\UserScript.ps1
Output file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\Output.tmp
```

```
Error file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\Err.tmp
```

Archivos de salida para la tarea **executeScript**

UserScript.*ext*

Contiene el script en el que se ejecutó la tarea `executeScript`. La extensión del archivo depende del tipo de script que haya especificado en el parámetro `type` de la tarea `executeScript`, como se indica a continuación:

- Si el tipo es `batch`, entonces la extensión del archivo es `.bat`.
- Si el tipo es `powershell`, entonces la extensión del archivo es `.ps1`.

Output.tmp

Contiene la salida del tiempo de ejecución del script en el que se ejecuta la tarea `executeScript`.

Err.tmp

Contiene el error del tiempo de ejecución del script en el que se ejecuta la tarea `executeScript`.

Ejemplos

En los siguientes ejemplos, se muestra cómo ejecutar un script en línea con la tarea `executeScript`.

Ejemplo 1: Archivo de texto de salida de Hola mundo

En este ejemplo, se muestra una tarea `executeScript` en la que se ejecuta un script de PowerShell para crear un archivo de texto que diga “Hola mundo” en la unidad `C:`.

```
task: executeScript
inputs:
- frequency: always
  type: powershell
  runAs: admin
  content: |-
    New-Item -Path 'C:\PowerShellTest.txt' -ItemType File
    Set-Content 'C:\PowerShellTest.txt' "Hello world"
```

Ejemplo 2: Ejecutar dos scripts

En este ejemplo, se muestra que la tarea `executeScript` puede ejecutar más de un script y que el tipo de script no tiene por qué coincidir.

El primer script (`type: powershell`) escribe un resumen de los procesos que se están ejecutando actualmente en la instancia en un archivo de texto ubicado en la unidad `C:`.

El segundo script (`batch`) escribe la información del sistema en el archivo `Output.tmp`.

```
task: executeScript
inputs:
- frequency: always
  type: powershell
  content: |
    Get-Process | Out-File -FilePath C:\Process.txt
  runAs: localSystem
- frequency: always
  type: batch
  content: |
    systeminfo
```

Ejemplo 3: Configurar el sistema idempotente con reinicios

En este ejemplo, se muestra una tarea `executeScript` en la que se ejecuta un script idempotente para realizar la siguiente configuración del sistema con un reinicio entre cada paso:

- Cambiar el nombre del equipo.
- Unir el equipo al dominio.
- Habilitar Telnet.

El script garantiza que cada operación se ejecute una sola vez. Esto evita un bucle de reinicio y hace que el script sea idempotente.

```
task: executeScript
inputs:
- frequency: always
  type: powershell
  runAs: localSystem
  content: |-
    $name = $env:ComputerName
     if ($name -ne $desiredName) {
       Rename-Computer -NewName $desiredName
```

```
    exit 3010
  }
  $domain = Get-ADDomain
  if ($domain -ne $desiredDomain)
  {
    Add-Computer -DomainName $desiredDomain
    exit 3010
  }
$telnet = Get-WindowsFeature -Name Telnet-Client
if (-not $telnet.Installed)
{
  Install-WindowsFeature -Name "Telnet-Client"
  exit 3010
}
```

extendRootPartition

Extiende el volumen raíz para utilizar todo el espacio disponible en el disco.

Frecuencia: una vez

AllowedStages — `[Boot]`

Entradas: ninguna

Ejemplo

```
task: extendRootPartition
```

initializeVolume

Inicializa los volúmenes vacíos que están asociados a la instancia para que se activen y se particionen. El agente de inicialización omite la inicialización si detecta que el volumen no está vacío. Un volumen se considera vacío si los primeros 4 KB del volumen están vacíos o si el volumen no tiene un diseño de unidad reconocible por Windows.

El parámetro de entrada `letter` siempre se aplica cuando se ejecuta esta tarea, independientemente de si la unidad ya está inicializada.

La tarea `initializeVolume` realiza las siguientes acciones.

- Establezca los atributos del disco `offline` y `readonly` en false.

- Cree una partición. Si no se especifica ningún tipo de partición en el parámetro de entrada `partition`, se aplican los siguientes valores predeterminados:
  - Si el tamaño del disco es inferior a 2 TB, defina el tipo de partición en `mbr`.
  - Si el tamaño del disco es de 2 TB o mayor, defina el tipo de partición en `gpt`.
- Dé formato al volumen como NTFS.
- Defina la etiqueta de volumen de la siguiente manera:
  - Use el valor del parámetro de entrada `name`, si procede.
  - Si el volumen es efímero y no se especificó ningún nombre, defina la etiqueta de volumen en `Temporary Storage Z`.
- Si el volumen es efímero (SSD o HDD, no Amazon EBS), cree un archivo `Important.txt` en la raíz del volumen con el siguiente contenido:

```
This is an 'Instance Store' disk and is provided at no additional charge.

*This disk offers increased performance since it is local to the host
*The number of Instance Store disks available to an instance vary by instance type
*DATA ON THIS DRIVE WILL BE LOST IN CASES OF IMPAIRMENT OR STOPPING THE INSTANCE.
 PLEASE ENSURE THAT ANY IMPORTANT DATA IS BACKED UP FREQUENTLY

For more information, please refer to: Almacén de instancias Amazon EC2.
```

- Defina la letra de la unidad en el valor especificado en el parámetro de entrada `letter`.

Etapas: puede ejecutar la tarea `initializeVolume` durante las etapas `PostReady` y `UserData`.

Frecuencia: siempre.

Entradas

Puede configurar los parámetros de tiempo de ejecución de la siguiente manera:

devices (lista de asignaciones)

(Condicional) Configuración para cada dispositivo que inicialice el agente de inicialización. Es necesario cuando el parámetro de entrada `initialize` se establece en `devices`.

- device (cadena, obligatorio): identifica el dispositivo durante la creación de la instancia. Por ejemplo, `xvdb`, `xvdf` o `\dev\nvme0n1`.
- letter (cadena, opcional): un carácter. La letra de unidad que se va a asignar.

- name (cadena, opcional): el nombre del volumen que se va a asignar.
- partition (cadena, opcional): especifique uno de los siguientes valores para el tipo de partición que desee crear o deje que el agente de inicialización tome el valor predeterminado en función del tamaño del volumen:
  - mbr
  - gpt

initialize (cadena)

(Obligatorio) Especifique exactamente uno de los siguientes valores:

- `all`
- `devices`

Ejemplos

En los siguientes ejemplos se muestran ejemplos de configuraciones de entrada para la tarea `initializeVolume`.

Ejemplo 1: inicializar dos volúmenes en una instancia

En este ejemplo, se muestra una tarea `initializeVolume` que inicializa dos volúmenes secundarios en una instancia. El dispositivo llamado `DataVolume2` en el ejemplo es efímero.

```
task: initializeVolume
inputs:
  initialize: devices
  devices:
  - device: xvdb
    name: DataVolume1
    letter: D
    partition: mbr
  - device: /dev/nvme0n1
    name: DataVolume2
    letter: E
    partition: gpt
```

Ejemplo 2: inicializar volúmenes de EBS adjuntos a una instancia

En este ejemplo, se muestra una tarea `initializeVolume` que inicializa todos los volúmenes vacíos de EBS adjuntos a la instancia.

```
task: initializeVolume
inputs:
  initialize: all
```

optimizeEna

Optimiza la configuración de ENA en función del tipo de instancia actual; podría reiniciar la instancia.

Frecuencia: siempre

AllowedStages — `[PostReady, UserData]`

Entradas: ninguna

Ejemplo

```
task: optimizeEna
```

setAdminAccount

Establece atributos para la cuenta de administrador predeterminada que se crea en el equipo local.

Frecuencia: una vez

AllowedStages — `[PreReady]`

Entradas —

`name`: (cadena) nombre de la cuenta de administrador

`password`: (mapa)

`type`: (cadena) estrategia para establecer la contraseña, ya sea como `static`, `random` o `doNothing`

`data`: (cadena) almacena datos si el campo `type` es estático

Ejemplo

```
task: setAdminAccount
inputs:
  name: Administrator
  password:
    type: random
```

setDnsSuffix

Agrega sufijos DNS a la lista de sufijos de búsqueda. Sólo se agregan a la lista los sufijos que aún no existen. Para obtener más información acerca de cómo los agentes de inicialización configuran los sufijos de DNS, consulte Configuración del sufijo de DNS para los agentes de inicialización de Windows.

Frecuencia: siempre

AllowedStages — `[PreReady]`

Entradas —

`suffixes`: (lista de cadenas) enumera uno o varios sufijos DNS válidos; las variables de sustitución válidas son `$REGION` y `$AZ`

Ejemplo

```
task: setDnsSuffix
inputs:
  suffixes:
  - $REGION.ec2-utilities.amazonaws.com
```

setHostName

Establece el nombre de host del equipo en una cadena personalizada o, si no se especifica `hostName`, la dirección IPv4 privada.

Frecuencia: siempre

AllowedStages — `[PostReady, UserData]`

Entradas —

`hostName`: (cadena) nombre de host opcional, que debe tener el siguiente formato.

- Debe tener 15 caracteres o menos
- Debe contener sólo caracteres alfanuméricos (a-z, A-Z, 0-9) y guión (-).
- No debe estar compuesta únicamente por caracteres numéricos.

`reboot`: (booleano) indica si se permite un reinicio cuando se cambia el nombre de host

Ejemplo

```
task: setHostName
inputs:
  reboot: true
```

setWallpaper

Crea el archivo de acceso directo `setwallpaper.lnk` en la carpeta de inicio de cada usuario existente, excepto el `Default User`. Este archivo de acceso directo se ejecuta cuando el usuario inicia sesión por primera vez después del arranque de la instancia. Configura la instancia con un fondo de pantalla personalizado que muestra los atributos de la instancia.

La ruta del archivo de acceso directo es:

```
$env:SystemDrive/Users/<user>/AppData/Roaming/Microsoft/Windows/Start Menu/Programs/
Startup/setwallpaper.lnk
```

> **Note**
>
> Al quitar la tarea `setWallpaper`, no elimina este archivo de acceso directo. Para obtener más información, consulte La tarea `setWallpaper` no está habilitada pero el fondo de pantalla se restablece al reiniciar.

Etapas: puede configurar el fondo de pantalla durante las etapas `PreReady` y `UserData`.

Frecuencia: `always`

Configuración de fondo de pantalla

Puede utilizar los siguientes ajustes para configurar su fondo de pantalla.

Entradas

Introduzca los parámetros que proporcione y los atributos que puede configurar para configurar el fondo de pantalla:

atributos (lista de cadenas)

(Opcional) Puede agregar uno o más de los siguientes atributos a su fondo de pantalla:

- `architecture`

- `availabilityZone`
- `hostName`
- `instanceId`
- `instanceSize`
- `memory`
- `network`
- `privateIpAddress`
- `publicIpAddress`

instanceTags

(Opcional) Puede utilizar exactamente una de las opciones siguientes para esta configuración.

- AllTags (cadena) (Todas las etiquetas): agregue todas las etiquetas de instancia a su fondo de pantalla.

```
instanceTags: AllTags
```

- InstanceTags (lista de cadenas) (Etiquetas de instancias): especifica una lista de nombres de etiquetas de instancia para agregarlos al fondo de pantalla. Por ejemplo:

```
instanceTags:
  - Tag 1
  - Tag 2
```

ruta (cadena)

(Obligatorio) La ruta del nombre del archivo de imagen local en formato .jpg que se va a utilizar en la imagen de fondo de pantalla.

Ejemplo

El siguiente ejemplo muestra las entradas de configuración del fondo de pantalla que establecen la ruta del archivo de la imagen de fondo del fondo de pantalla, junto con las etiquetas de instancia denominadas `Tag 1` y `Tag 2`, y los atributos que incluyen el nombre de host, el ID de la instancia y las direcciones IP públicas y privadas de la instancia.

```
task: setWallpaper
inputs:
```

```
  path: C:\ProgramData\Amazon\EC2Launch\wallpaper\Ec2Wallpaper.jpg
  attributes:
  - hostName
  - instanceId
  - privateIpAddress
  - publicIpAddress
  instanceTags:
  - Tag 1
  - Tag 2
```

> **Note**
>
> Debe habilitar las etiquetas en los metadatos para que se muestren en el fondo de pantalla. Para obtener más información acerca de las etiquetas y metadatos de instancias, consulte Trabajar con etiquetas de instancia en los metadatos de instancia.

startSsm

Comienza el servicio Systems Manager (SSM) siguiendo Sysprep.

Frecuencia: siempre

AllowedStages — `[PostReady, UserData]`

Entradas: ninguna

Ejemplo

```
task: startSsm
```

sysprep

Restablece el estado del servicio, actualiza `unattend.xml`, desactiva RDP y ejecuta Sysprep. Esta tarea sólo se ejecuta después de que se hayan completado todas las demás tareas.

Frecuencia: una vez

AllowedStages — `[UserData]`

Entradas —

`clean`: (booleano) limpia los registros de instancia antes de ejecutar Sysprep

`shutdown`: (booleano) cierra la instancia después de ejecutar Sysprep

Ejemplo

```
task: sysprep
inputs:
  clean: true
  shutdown: true
```

writeFile

Escribe un archivo en un destino.

Frecuencia: consulte Entradas

AllowedStages — `[PostReady, UserData]`

Entradas —

`frequency`: (cadena) uno entre `once` y `always`

`destination`: (cadena) ruta en la que escribir el contenido

`content`: (cadena) texto para escribir en el destino

Ejemplo

```
task: writeFile
inputs:
- frequency: once
  destination: C:\Users\Administrator\Desktop\booted.txt
  content: Windows Has Booted
```

Códigos de salida y reinicios de EC2Launch v2

Puede utilizar EC2Launch v2 para definir cómo los scripts manejan los códigos de salida. De forma predeterminada, el código de salida del último comando ejecutado en un script se registra como el código de salida de todo el script. Por ejemplo, si una secuencia de comandos incluye tres comandos y el primer comando falla pero los siguientes se ejecutan correctamente, el estado de ejecución se informa como `success` porque el comando final se ha realizado correctamente.

Si desea que un script reinicie una instancia, debe especificar el `exit 3010` en el script, incluso cuando el reinicio sea el último paso del script. `exit 3010` indica a EC2Launch v2 que reinicie

la instancia y llame nuevamente al script hasta que devuelva un código de salida que no sea `3010`, o hasta que se haya alcanzado el número máximo de reinicios. EC2Launch v2 permite un máximo de 5 reinicios por tarea. Si intentas reiniciar una instancia desde un script utilizando un mecanismo diferente, como por ejemplo `Restart-Computer`, el estado de ejecución del script será incoherente. Por ejemplo, puede quedarse atascado en un bucle de reinicio o no realizar el reinicio.

Si utiliza un formato de datos de usuario XML que es compatible con agentes antiguos, los datos de usuario pueden ejecutarse más veces de las que desea. Para obtener más información, consulte El servicio ejecuta datos de usuario más de una vez en la sección de resolución de problemas.

EC2Launch v2 y Sysprep

El servicio EC2Launch v2 ejecuta Sysprep, una herramienta de Microsoft que le permite crear una AMI de Windows personalizada que se puede reutilizar. Cuando EC2Launch v2 llama a Sysprep, utiliza los archivos de `%ProgramData%\Amazon\EC2Launch` para determinar qué operaciones realizar. Puede editar estos archivos de manera indirecta mediante el cuadro de diálogo Configuración de EC2Launch o directamente mediante un editor YAML o un editor de texto. Sin embargo, hay algunas opciones de configuración avanzada que no están disponibles en el cuadro de diálogo Configuración de EC2Launch, por lo que debe editar dichas entradas directamente.

Si crea una AMI desde una instancia después de actualizar su configuración, la nueva configuración se aplica a cualquier instancia que se lance desde la nueva AMI. Para obtener información acerca de la creación de una AMI, consulte Creación de una AMI basada en Amazon EBS.

Solucionar problemas de EC2Launch v2

En esta sección, se muestran escenarios de solución de problemas comunes para EC2Launch v2, información sobre cómo ver los registros de eventos de Windows y los mensajes y la salida del registro de la consola.

Solución de problemas de temas

- Situaciones comunes de solución de problemas
- Registros de eventos de Windows
- Salida del registro de la consola de EC2Launch v2

Situaciones comunes de solución de problemas

En esta sección se muestran las situaciones comunes de solución de problemas y los pasos para la resolución.

Situaciones

- El servicio no puede configurar el fondo de pantalla
- El servicio no puede ejecutar datos de usuario
- El servicio ejecuta una tarea sólo una vez
- El servicio no puede ejecutar una tarea
- El servicio ejecuta datos de usuario más de una vez
- Las tareas programadas de EC2Launch v1 no se pueden ejecutar después de la migración a EC2Launch v2
- El servicio inicializa un volumen EBS que no está vacío
- La tarea setWallpaper no está habilitada pero el fondo de pantalla se restablece al reiniciar
- Servicio atascado en estado de ejecución
- agent-config.yml no válido impide que se abra el cuadro de diálogo de configuración de EC2Launch v2
- task:executeScript should be unique and only invoked once

El servicio no puede configurar el fondo de pantalla

Resolución

1. Compruebe que `%AppData%\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\setwallpaper.lnk` existe.
2. Compruebe `%ProgramData%\Amazon\EC2Launch\log\agent.log` si se ha producido algún error.

El servicio no puede ejecutar datos de usuario

Causa posible: el servicio puede haber devuelto un error antes de ejecutar los datos de usuario.

Resolución

1. Compruebe `%ProgramData%\Amazon\EC2Launch\state\previous-state.json`.
2. Compruebe si `boot`, `network`, `preReady` y `postReadyLocalData` se han marcado como éxito.
3. Si una de las etapas devolvió un error, compruebe si hay errores específicos en `%ProgramData%\Amazon\EC2Launch\log\agent.log`.

El servicio ejecuta una tarea sólo una vez

Resolución

1. Compruebe la frecuencia de la tarea.
2. Si el servicio ya se ejecutó después de Sysprep y la frecuencia de la tarea está establecida en `once`, la tarea no se ejecutará de nuevo.
3. Configure la frecuencia de la tarea como `always` si desea que se ejecute cada vez que se ejecute EC2Launch v2.

El servicio no puede ejecutar una tarea

Resolución

1. Compruebe las últimas entradas en `%ProgramData%\Amazon\EC2Launch\log\agent.log`.
2. Si no se han producido errores, pruebe a ejecutar el servicio manualmente desde `"%ProgramFiles%\Amazon\EC2Launch\EC2Launch.exe" run` para ver si las tareas se realizan correctamente.

El servicio ejecuta datos de usuario más de una vez

Resolución

Los datos de usuario se gestionan de forma diferente entre EC2Launch v1 y EC2Launch v2. EC2Launch v1 ejecuta los datos de usuario como una tarea programada en la instancia cuando configura `persist` como `true`. Si `persist` se establece en `false`, la tarea no está programada incluso cuando se cierra con un reinicio o se interrumpe mientras se ejecuta.

EC2Launch v2 ejecuta los datos de usuario como una tarea de agente y realiza un seguimiento de su estado de ejecución. Si los datos de usuario emiten un reinicio del equipo o si los datos de usuario se interrumpieron durante la ejecución, el estado de ejecución persiste como `pending` y los datos de usuario se ejecutarán de nuevo en el siguiente arranque de la instancia. Si deseas evitar que el script de datos del usuario se ejecute más de una vez, haz que el script sea idempotente.

El siguiente ejemplo de scripts idempotentes establece el nombre del equipo y se une a un dominio.

```
<powershell>
  $name = $env:computername
```

```
  if ($name -ne $desiredName) {
 Rename-Computer -NewName $desiredName
  }
  $domain = Get-ADDomain
  if ($domain -ne $desiredDomain)
  {
 Add-Computer -DomainName $desiredDomain
  }
  $telnet = Get-WindowsFeature -Name Telnet-Client
  if (-not $telnet.Installed)
  {
 Install-WindowsFeature -Name "Telnet-Client"
  }
</powershell>
<persist>false</persist>
```

Las tareas programadas de EC2Launch v1 no se pueden ejecutar después de la migración a EC2Launch v2

Resolución

La herramienta de migración no detecta ninguna tarea programada que esté vinculada a scripts de EC2Launch v1; por lo tanto, no configura automáticamente dichas tareas en EC2Launch v2. Para configurar dichas tareas, edita el archivo `agent-config.yml` o utiliza el Cuadro de diálogo configuración de EC2Launch v2. Por ejemplo, si una instancia tiene una tarea programada que ejecuta `InitializeDisks.ps1`, después de ejecutar la herramienta de migración debe especificar los volúmenes que desea iniciar en el cuadro de diálogo configuración de EC2Launch v2. Consulte el paso 6 del procedimiento para Cambiar la configuración mediante el cuadro de diálogo de configuración de EC2Launch v2.

El servicio inicializa un volumen EBS que no está vacío

Resolución

Antes de inicializar un volumen, EC2Launch v2 intenta detectar si está vacío. Si un volumen no está vacío, omite la inicialización. Los volúmenes que se detecten como no vacíos no se inicializan. Un volumen se considera vacío si los primeros 4 KB de un volumen están vacíos, o si un volumen no tiene un diseño de unidad reconocible por Windows. Un volumen que se inicializó y formateó en un sistema Linux no tiene un diseño de unidad reconocible por Windows, por ejemplo MBR o GPT. Por lo tanto, se considerará vacío e inicializado. Si desea conservar estos datos, no dependa de la detección de unidades vacías de EC2Launch v2. En lugar de ello, especifique los volúmenes que

desea inicializar en el cuadro de diálogo de configuración de EC2Launch v2 (consulte el paso 6) o en `agent-config.yml`.

La tarea **`setWallpaper`** no está habilitada pero el fondo de pantalla se restablece al reiniciar

La tarea `setWallpaper` crea el archivo de acceso directo `setwallpaper.lnk` en la carpeta de inicio de cada usuario existente, excepto el `Default User`. Este archivo de acceso directo se ejecuta cuando el usuario inicia sesión por primera vez después del arranque de la instancia. Configura la instancia con un fondo de pantalla personalizado que muestra los atributos de la instancia. Tenga en cuenta que quitar la tarea `setWallpaper` no elimina este archivo de acceso directo. Elimine manualmente este archivo o mediante un script.

La ruta del acceso directo es:

`$env:SystemDrive/Users/<user>/AppData/Roaming/Microsoft/Windows/Start Menu/Programs/Startup/setwallpaper.lnk`

Resolución

Elimine manualmente este archivo o mediante un script.

Ejemplo de script de PowerShell para eliminar un archivo de acceso directo

```
foreach ($userDir in (Get-ChildItem "C:\Users" -Force -Directory).FullName)
{
 $startupPath = Join-Path $userDir -ChildPath "AppData\Roaming\Microsoft\Windows\Start
 Menu\Programs\Startup"
 if (Test-Path $startupPath)
 {
  $wallpaperSetupPath = Join-Path $startupPath -ChildPath "setwallpaper.lnk"
  if (Test-Path $wallpaperSetupPath)
  {
   Remove-Item $wallpaperSetupPath -Force -Confirm:$false
  }
 }
}
```

Servicio atascado en estado de ejecución

Descripción

EC2Launch v2 se bloquea y presenta mensajes de registro (`agent.log`) similares a los siguientes:

```
2022-02-24 08:08:58 Info:
 ********************************************************************************
2022-02-24 08:08:58 Info: EC2Launch Service starting
2022-02-24 08:08:58 Info: Windows event custom log exists: Amazon EC2Launch
2022-02-24 08:08:58 Info: ACPI SPCR table not supported. Bailing Out
2022-02-24 08:08:58 Info: Serial port is in use. Waiting for Serial Port...
2022-02-24 08:09:00 Info: ACPI SPCR table not supported. Use default console port.
2022-02-24 08:09:02 Info: ACPI SPCR table not supported. Use default console port.
2022-02-24 08:09:04 Info: ACPI SPCR table not supported. Use default console port.
2022-02-24 08:09:06 Info: ACPI SPCR table not supported. Use default console port.
```

Causa posible

SAC está habilitado y utiliza el puerto serie. Para obtener más información, consulte Usar SAC para solucionar problemas de su instancia de Windows.

Resolución

Pruebe los siguientes pasos para resolver este problema:

- Desactive el servicio que esté utilizando el puerto serie.
- Si desea que el servicio siga utilizando el puerto serie, escriba scripts personalizados para realizar tareas del agente de inicialización e invóquelas como tareas programadas.

`agent-config.yml` no válido impide que se abra el cuadro de diálogo de configuración de EC2Launch v2

Descripción

La configuración de EC2Launch v2 intenta analizar el archivo `agent-config.yml` antes de abrir el cuadro de diálogo. Si el archivo de configuración YAML no sigue el esquema admitido, el cuadro de diálogo mostrará el siguiente error:

```
Unable to parse configuration file agent-config.yml. Review configuration
file. Exiting application.
```

Resolución

1. Compruebe que el archivo de configuración sigue el esquema admitido.

2. Si desea comenzar desde cero, copie el archivo de configuración predeterminado en `agent-config.yml`. Puede utilizar el ejemplo `agent-config.yml` que se proporciona en la sección Task Configuration (Configuración de tareas).
3. También puede comenzar de nuevo eliminando `agent-config.yml`. La configuración de EC2Launch v2 genera un archivo de configuración vacío.

`task:executeScript should be unique and only invoked once`

Descripción

No es posible repetir una tarea en la misma etapa.

Resolución

Algunas tareas deben introducirse como una matriz, como executeScript y executeProgram. Para ver un ejemplo de cómo escribir el script como una matriz, consulte executeScript.

Registros de eventos de Windows

EC2Launch v2 publica registros de eventos de Windows para eventos importantes, como el inicio del servicio, la preparación de Windows para empezar a funcionar y el éxito y el error de la tarea. Los identificadores de eventos identifican de forma única un evento en particular. Cada evento contiene información de etapa, tarea y nivel, así como una descripción. Puede establecer desencadenadores para eventos específicos mediante el identificador de evento.

Los ID de eventos proporcionan información sobre un evento e identifican de forma única algunos eventos. El dígito menos significativo de un ID de evento indica la gravedad de un evento.

Evento	Dígito menos significativo
`Success`	`. . .0`
`Informational`	`. . .1`
`Warning`	`. . .2`
`Error`	`. . .3`

Los eventos relacionados con el servicio que se generan cuando se inicia o se detiene el servicio incluyen un identificador de evento de un solo dígito.

Evento	Identificador de un solo dígito
`Success`	`0`
`Informational`	`1`
`Warning`	`2`
`Error`	`3`

Los mensajes de eventos para eventos `EC2LaunchService.exe` comienzan por `Service:`. Los mensajes de eventos para eventos `EC2Launch.exe` no comienzan por `Service:`.

Los ID de eventos de cuatro dígitos incluyen información sobre la fase, la tarea y la gravedad de un evento.

Temas

- Formato de ID de evento
- Ejemplos de ID de evento
- Esquema de registro de eventos de Windows

Formato de ID de evento

La siguiente tabla muestra el formato del identificador de un evento de EC2Launch v2.

3	2 1	0
S	T	L

Las letras y números de la tabla representan el tipo de evento y las definiciones siguientes.

Tipo de evento	Definición
S (Etapa)	0 - Mensaje de nivel de servicio

Tipo de evento	Definición
	1 - Arranque 2 - Red 3 - Pre-Ready 5 - Windows está listo 6 - PostReady 7 - Datos de usuario
T (Tarea)	Las tareas representadas por los dos valores correspondientes son distintas para cada etapa. Para ver la lista completa de eventos, consulte Esquema de registro de eventos de Windows.
L (Nivel del evento)	0 - Éxito 1 - Informativo 2 - Advertencia 3 - Error

Ejemplos de ID de evento

A continuación se presentan identificadores de evento de ejemplo.

- `5000`: Windows está listo para usar
- `3010`: la tarea de activación de Windows en la etapa PreReady se ha realizado correctamente
- `6013`: la tarea Establecer fondo de pantalla en la etapa PostReady Local Data encontró un error

Esquema de registro de eventos de Windows

ID de mensaje/evento	Mensaje de evento
. . .0	Success
. . .1	Informational
. . .2	Warning
. . .3	Error
x	EC2Launch service-level logs
0	EC2Launch service exited successfully
1	EC2Launch service informational logs
2	EC2Launch service warning logs
3	EC2Launch service error logs
10	Replace state.json with previous-state.json
100	Serial Port
200	Sysprep
300	PrimaryNic
400	Metadata
x000	Stage (1 digit), Task (2 digits), Status (1 digit)
1000	Boot
1010	Boot - extend_root_partition

ID de mensaje/evento	Mensaje de evento
2000	Network
2010	Network - add_routes
3000	PreReady
3010	PreReady - activate_windows
3020	PreReady - install_egpu_manager
3030	PreReady - set_monitor_on
3040	PreReady - set_hibernation
3050	PreReady - set_admin_account
3060	PreReady - set_dns_suffix
3070	PreReady - set_wallpaper
3080	PreReady - set_update_schedule
3090	PreReady - output_log
3100	PreReady - enable_open_ssh
5000	Windows is Ready to use
6000	PostReadyLocalData
7000	PostReadyUserData
6010/7010	PostReadyLocal/UserData - set_wallpaper
6020/7020	PostReadyLocal/UserData - set_update_schedule

ID de mensaje/evento	Mensaje de evento
6030/7030	PostReadyLocal/UserData - set_hostname
6040/7040	PostReadyLocal/UserData - execute_program
6050/7050	PostReadyLocal/UserData - execute_script
6060/7060	PostReadyLocal/UserData - manage_package
6070/7070	PostReadyLocal/UserData - initialize_volume
6080/7080	PostReadyLocal/UserData - write_file
6090/7090	PostReadyLocal/UserData - start_ssm
7100	PostReadyUserData - enable_open_ssh
6110/7110	PostReadyLocal/UserData - enable_jumbo_frames

Salida del registro de la consola de EC2Launch v2

Esta sección contiene una salida del registro de la consola de ejemplo de EC2Launch v2 y muestra todos los mensajes de error del registro de la consola de EC2Launch v2 para ayudarle a solucionar problemas. Para obtener más información sobre la salida de la consola de instancias y cómo acceder a ella, consulte the section called “Salida de la consola de instancias”.

Salidas

- Salida del registro de la consola de EC2Launch v2

- Mensajes de registro de la consola de EC2Launch v2

Salida del registro de la consola de EC2Launch v2

A continuación, se muestra una salida del registro de la consola de ejemplo de EC2Launch v2.

```
2023/11/30 20:18:53Z: Windows sysprep configuration complete.
2023/11/30 20:18:57Z: Message: Waiting for access to metadata...
2023/11/30 20:18:57Z: Message: Meta-data is now available.
2023/11/30 20:18:57Z: AMI Origin Version: 2023.11.15
2023/11/30 20:18:57Z: AMI Origin Name: Windows_Server-2022-English-Full-Base
2023/11/30 20:18:58Z: OS: Microsoft Windows NT 10.0.20348
2023/11/30 20:18:58Z: OsVersion: 10.0
2023/11/30 20:18:58Z: OsProductName: Windows Server 2022 Datacenter
2023/11/30 20:18:58Z: OsBuildLabEx: 20348.1.amd64fre.fe_release.210507-1500
2023/11/30 20:18:58Z: OsCurrentBuild: 20348
2023/11/30 20:18:58Z: OsReleaseId: 2009
2023/11/30 20:18:58Z: Language: en-US
2023/11/30 20:18:58Z: TimeZone: UTC
2023/11/30 20:18:58Z: Offset: UTC +0000
2023/11/30 20:18:58Z: Launch: EC2 Launch v2.0.1643
2023/11/30 20:18:58Z: AMI-ID: ami-1234567890abcdef1
2023/11/30 20:18:58Z: Instance-ID: i-1234567890abcdef0
2023/11/30 20:18:58Z: Instance Type: c5.large
2023/11/30 20:19:00Z: Driver: AWS NVMe Driver v1.5.0.33
2023/11/30 20:19:00Z: SubComponent: AWS NVMe Driver v1.5.0.33;
 EnableSCSIPersistentReservations: 0
2023/11/30 20:19:00Z: Driver: AWS PV Driver Package v8.4.3
2023/11/30 20:19:01Z: Driver: Amazon Elastic Network Adapter v2.6.0.0
2023/11/30 20:19:01Z: RDPCERTIFICATE-SUBJECTNAME: EC2AMAZ-SO1T009
2023/11/30 20:19:01Z: RDPCERTIFICATE-THUMBPRINT:
 1234567890ABCDEF1234567890ABCDEF1234567890
2023/11/30 20:19:09Z: SSM: Amazon SSM Agent v3.2.1705.0
2023/11/30 20:19:13Z: Username: Administrator
2023/11/30 20:19:13Z: Password: <Password>
1234567890abcdef1EXAMPLEPASSWORD
</Password>
2023/11/30 20:19:14Z: User data format: no_user_data
2023/11/30 20:19:14Z: EC2LaunchTelemetry: IsTelemetryEnabled=true
2023/11/30 20:19:14Z: EC2LaunchTelemetry: AgentOsArch=windows_amd64
2023/11/30 20:19:14Z: EC2LaunchTelemetry: IsAgentScheduledPerBoot=true
2023/11/30 20:19:14Z: EC2LaunchTelemetry: AgentCommandErrorCode=0
```

```
2023/11/30 20:19:14Z: Message: Windows is Ready to use
```

Mensajes de registro de la consola de EC2Launch v2

A continuación, se muestra una lista de todos los mensajes de registro de la consola de EC2Launch v2.

```
Message: Error EC2Launch service is stopping. {error message}
 Error setting up EC2Launch agent folders
 See instance logs for detail
 Error stopping service
 Error initializing service
Message: Windows sysprep configuration complete
Message: Invalid administrator username: {invalid username}
Message: Invalid administrator password
Username: {username}
Password: <Password>{encrypted password}</Password>
AMI Origin Version: {amiVersion}
AMI Origin Name: {amiName}
Microsoft Windows NT {currentVersion}.{currentBuildNumber}
OsVersion: {currentVersion}
OsProductName: {productName}
OsBuildLabEx: {buildLabEx}
OsCurrentBuild: {currentBuild}
OsReleaseId: {releaseId}
Language: {language}
TimeZone: {timeZone}
Offset: UTC {offset}
Launch agent: EC2Launch {BuildVersion}
AMI-ID: {amiId}
Instance-ID: {instanceId}
Instance Type: {instanceType}
RDPCERTIFICATE-SUBJECTNAME: {certificate subject name}
RDPCERTIFICATE-THUMBPRINT: {thumbprint hash}
SqlServerBilling: {sql billing}
SqlServerInstall: {sql patch leve, edition type}
Driver: AWS NVMe Driver {version}
Driver: Inbox NVMe Driver {version}
Driver: AWS PV Driver Package {version}
Microsoft-Hyper-V is installed.
Unable to get service status for vmms
Microsoft-Hyper-V is {status}
SSM: Amazon SSM Agent {version}
```

```
AWS VSS Version: {version}
Message: Windows sysprep configuration complete
Message: Windows is being configured. SysprepState is {state}
Windows is still being configured. SysprepState is {state}
Message: Windows is Ready to use
Message: Waiting for meta-data accessibility...
Message: Meta-data is now available.
Message: Still waiting for meta-data accessibility...
Message: Failed to find primary network interface...retrying...
User data format: {format}
```

Historiales de versiones de EC2Launch v2

Historiales de versiones

- Historial de versiones de EC2Launch v2
- Historial de versiones de la herramienta de migración de EC2Launch v2

Historial de versiones de EC2Launch v2

En la siguiente tabla, se describen las versiones de EC2Launch v2 publicadas.

Versión	Detalles	Fecha de la versión
2.0.1924	• Se actualizó la interfaz de usuario de EC2Launch Settings. • Se actualizó el comando de la CLI del fondo de pantalla. • Se actualizó el instalador de EC2Launch.	10 de junio de 2024
2.0.1914	• Agregue rutas con direcciones de puerta de enlace no especificadas (`0.0.0.0` para IPv4 o `::` para IPv6). • Siempre agregue rutas IPv4 e IPv6. • Se ha corregido un problema por el que el nombre de usuario `Administrator` se agregó al archivo `agent-config.yml` cuando no se especificaba.	5 de junio de 2024

Versión	Detalles	Fecha de la versión
	• Permisos modificados de EC2Launch v2.	
2.0.1881	• Se agregó una opción de contraseña cifrada a la tarea `setAdminAccount` . • Se agregó el comando de la CLI para cifrar la contraseña estática en agent-config.yml. • Se corrigió el problema de que los datos de usuario de XML no incluían los argumentos de PowerShell al ejecutarse con permisos de administrador. Para obtener más información, consulte Cómo gestiona Amazon EC2 los datos de usuario de las instancias de Windows. • Se ajustaron los argumentos de PowerShell para la tarea `executeScript` y los scrips de datos de usuario al ejecutarse con permisos de `LocalSystem` . Cuando los argumentos están vacíos, el agente utiliza el siguiente valor predeterminado: `-ExecutionPolicy Unrestricted` . • Se evitó la impresión de versiones de controlador duplicadas en el registro de la consola.	8 de mayo de 2024

Versión	Detalles	Fecha de la versión
2.0.1815	• Se ajustó la gestión de errores para que produjera un error en los problemas críticos de configuración anteriores a sysprep. • Se ha corregido un problema que provocaba que las tareas de fondo de pantalla y nombre de host utilizaran una dirección IP incorrecta en instancias con varias direcciones IP asignadas a la interfaz de red principal. • Las tareas de fondo de pantalla y nombre de host se cambiaron para obtener primero la IP privada del IMDS y, luego, volver a WMI si el IMDS estaba desactivado. • Se ha corregido un problema en la tarea `initializeVolume` que provocaba que los volúmenes `sc1` no se inicializaran debido a un error transitorio.	6 de marzo de 2024
2.0.1739	• Se corrigió un error que impedía que las tareas de `executeScript` que se ejecutaban como usuario administrador de Windows capturaran los códigos de salida.	17 de enero de 2024

Versión	Detalles	Fecha de la versión
2.0.1702	• Se restringieron los permisos `Telemetry.log` para `read-execute` solo para usuarios estándar. • Se configuró el servicio EC2Launch para Windows para que se reiniciara en caso de un error de inicio. • Se permitió que los errores `add-routes` sean procesables al registrar la salida `route.exe stderr`. • Se corrigió un problema que se producía cuando las métricas de ruta estaban fuera del rango [1, 9999]. • Se agregó compatibilidad con fondos de escritorio para varios tipos de instancia nuevos. • Se corrigió un problema provocado por los scripts de datos de usuarios que se ejecutan como usuario administrador de Windows y que envían los resultados a `stderr`.	4 de enero de 2024

Versión	Detalles	Fecha de la versión
2.0.1643	• Se actualizó la herramienta `ebsnvme-id.exe` a la versión 1.1.0.7. • Se corrigió un problema con la configuración del escalado lateral de recepción (RSS) y de la profundidad de las colas de recepción en los tipos de instancias metal que comienzan por “metal-*”, como metal-48x1. • Se eliminó el evento de telemetría que informa sobre los comandos XML de datos de usuario que bloquean el agente. • Se actualizó la tarea `setDnsSuffix` para limitar la devolución de nombres de dominio en función de la entrada de registro: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters\DomainNameDevolutionLevel`. • Se agregó una tarea pública y una CLI que agrega rutas de red. • Nota: Esta es la última versión que es compatible oficialmente con Windows Server 2012. • Nota: Esta es la última versión que admite oficialmente los sistemas operativos de 32 bits.	4 de octubre de 2023

Versión	Detalles	Fecha de la versión
2.0.1580	• Se modificó la forma en que el agente de inicialización gestiona los errores al modificar los permisos del archivo de registro. • Se agregó un tiempo de espera para la conexión con el puerto de serie. El tiempo de espera permite que el agente de inicialización continúe en ejecución si el puerto de serie está en uso.	5 de septiembre de 2023

Versión	Detalles	Fecha de la versión

2.0.1521	• Se ha dejado obsoleto el indicador –`block` de los comandos `EC2Launch.exe` , reset y sysprep.
	• Se ha actualizado `EC2Launch.exe` para detectar y gestionar los comandos reset y sysprep que se utilizan en las tareas `executeScript` en línea. Estos comandos hacen que el agente deje de ejecutarse después de que la tarea `executeScript` los ejecute.
	• Se han actualizado los scripts XML de datos de usuario para que se ejecuten en línea de forma predeterminada.
	• Habilite los scripts de datos de usuario XML para que se ejecuten independientemente de la nueva etiqueta `detach`. Para obtener más información, consulte Scripts de datos de usuario.
	• Se hicieron los siguientes cambios en el registro del agente.
	  • Se actualizaron los mensajes de registro del agente.
	  • Se eliminó el contenido de y la salida de `executeScript` del registro del agente.
	  • Se eliminaron los argumentos y la salida de `executeProgram` del registro del agente.
	• Se hicieron los siguientes cambios en el registro de la consola.
	  • Se ha agregado el valor `EnableSCSIPersistentReservations` al registro de la consola.
		3 de julio de 2023

Versión	Detalles	Fecha de la versión
2.0.1303	• Se agregaron líneas de registro y gestión de errores adicionales al agregar rutas de red. • Tareas `executeScript` y `executeProgram` permitidas en la fase PreReady. • Se ha actualizado la tarea `executeProgram` para generar archivos de salida similares a los de la tarea executeScript. Para obtener más información, consulte executeProgram. • Se agregó telemetría para monitorear el uso de los comandos del agente de bloqueo en los datos de usuario XML.	3 de mayo de 2023
2.0.1245	• Se mejoró la visibilidad de los bloqueos al registrar las pilas de llamadas inesperadas en texto claro. • Se agregó el servicio EventLog como dependencia de inicio para corregir un bloqueo que se producía cuando el servicio Amazon EC2Launch se inicia más rápido que el servicio EventLog. • Se hizo que los datos de usuario en XML se ejecutaran antes de la etapa PostReady desde el archivo de configuración del agente (como EC2Launch v1 y EC2Config). • Se agregó la versión 1.1 de datos de usuario de YAML para que los datos de usuario se ejecuten antes de la etapa PostReady desde el archivo de configuración del agente (la versión 1.0 de datos de usuario de YAML se ejecuta después de la etapa PostReady desde el archivo de configuración del agente).	8 de marzo de 2023

Versión	Detalles	Fecha de la versión
2.0.1173	• Agrega una función opcional para mostrar las etiquetas de instancia en el fondo de pantalla. Para obtener más informaci ón, consulte setWallpaper . • Agrega la gestión de errores cuando el grupo de seguridad de Elastic Graphics no está configurado correctamente. • Corrige un tiempo de espera cuando el servicio de metadatos de instancia no está activado.	6 de febrero de 2023
2.0.1121	• Soluciona un problema por el que se imprimía un error 404 en el fondo de pantalla cuando no se asignaba ninguna dirección IPv4 pública. • Soluciona un problema por el que el sistema de archivos del volumen se formateaba como, `RAW` en lugar de `NTFS` cuando la letra de la unidad del dispositivo estaba configurada como `D`. • Soluciona un problema por el que los volúmenes SSD NVMe se identificaban incorrectamente como volúmenes de EBS. • Corrige un error al activar Windows cuando el IMDS está desactivado.	4 de enero de 2023

Versión	Detalles	Fecha de la versión
2.0.1082	• Soluciona un problema que provoca que el campo `setWallpaper : privateIpAddress` esté en blanco cuando IMDS está deshabilitado. • Soluciona un problema de configuración del nombre de host en la dirección IPv4 privada cuando IMDS está deshabilitado. • Soluciona un problema relacionado con la inicialización de volúmenes en Windows Server 2012. • Soluciona un problema relacionado con la configuración de marcos gigantes. • Soluciona un error que se producía cuando no se especific aba ninguna clave SSH al iniciar la instancia. • Soluciona un error en Windows Server 2012 cuando Windows no tiene una clave de registro “ReleaseID”.	7 de diciembre de 2022
2.0.1011	• Corrige la lógica para encontrar el adaptador de red cuando PnPDeviceID está vacío.	11 de noviembre de 2022
2.0.1009	• Utiliza la información del segmento PCI para seleccionar el puerto de la consola.	8 de noviembre de 2022

Versión	Detalles	Fecha de la versión
2.0.982	• Agrega lógica de reintentos para obtener información de RDP. • Corrige los errores durante la inicialización del volumen en las instancias `d2.8xlarge` . • Soluciona el problema por el que se puede seleccionar un adaptador de red incorrecto después de un reinicio. • Elimina el mensaje de error de falsa alarma cuando la SPCR de ACPI no está disponible.	31 de octubre de 2022
2.0.863	• Actualiza la lógica de espera de IMDS para realizar solo solicitudes IMDSv2. • Agrega lógica para asignar letras de unidad a volúmenes que ya están inicializados pero no montados. • Imprime un mensaje de error más específico cuando no se admite el tipo de par de claves. • Corrige el error de código de reinicio 3010. • Agrega comprobación para datos de usuario codificados con base64 no válidos.	6 de julio de 2022
2.0.698	• Corrige errores tipográficos en la salida del registro cuando se ejecutan scripts.	30 de enero de 2022

Versión	Detalles	Fecha de la versión
2.0.674	• La telemetría carga el control de privacidad habilitado o desactivado. • Corrige errores de `index out of bounds`. • Elimina los accesos directos del fondo de pantalla durante `sysprep`.	15 de noviembre de 2021
2.0.651	• Agrega lógica para desinstalar agentes heredados durante la instalación de EC2Launch v2. • Corrige el problema de la CLI `list-volume` cuando el volumen raíz no aparece como volumen 0.	7 de octubre de 2021
2.0.592	• Corrige un error para informar correctamente el estado de la etapa. • Elimina mensajes de error de falsa alarma cuando se cierran los archivos de registros. • Agrega telemetría.	31 de agosto de 2021
2.0.548	• Agrega ceros a la izquierda para el nombre de host IP hexadecimal. • Corrige permisos de archivo para la tarea `enableOpenSsh` . • Corrige el bloqueo del comando sysprep.	4 de agosto de 2021

Versión	Detalles	Fecha de la versión
2.0.470	• Corrige un error en la etapa de red para esperar a que DHCP asigne una IP a la instancia. • Correcciones de errores con `setDnsSuffix` cuando la clave de registro `SearchList` no existe. • Corrige un error en la lógica de devolución de DNS en `setDnsSuffix` . • Agrega rutas de red después de reinicios intermedios. • Permite a `initializeVolume` volver a escribir volúmenes existentes. • Elimina información adicional del subcomando de versión.	20 de julio de 2021
2.0.285	• Agrega la opción para ejecutar secuencias de comandos de usuario en un proceso desvinculado. • Los datos de usuario heredados (datos de usuario XML) ahora se ejecutan en un proceso desvinculado, que es un comportamiento similar al agente de inicialización anterior. • Agrega el indicador CLI a los comandos `sysprep` y `reset`, lo que les permite bloquearlos hasta que el servicio se detenga. • Restringe los permisos de la carpeta de configuración.	8 de marzo de 2021

Versión	Detalles	Fecha de la versión
2.0.207	• Agrega un campo opcional `hostName` a la tarea `setHostName` . • Corrige el error de reinicio. Reinicie las tareas `executeScript` y `executeProgram` se marcará como en ejecución. • Agrega más códigos de retorno al comando de estado. • Agrega el servicio de arranque para corregir el problema de inicio cuando se ejecuta en el tipo de instancia `t2.nano`. • Corrige el modo de instalación limpia para eliminar archivos no rastreados por el instalador.	2 de febrero de 2021
2.0.160	• Corrige el comando `validate` para detectar un nombre de etapa no válido. • Agrega el comando `w32tm resync` en la tarea `addroutes` . • Soluciona un problema al cambiar el orden de búsqueda de sufijos DNS. • Agrega condiciones de comprobación para informar mejor de los datos de usuario no válidos.	4 de diciembre de 2020
2.0.153	Agrega la funcionalidad de Sysprep en UserData.	3 de noviembre de 2020

Versión	Detalles	Fecha de la versión
2.0.146	• Corrige un problema con RootExtend en AMI no inglesas. • Otorga al grupo de usuarios permiso de escritura en archivos de registro. • Crea una partición reservada de MS para volúmenes GPT. • Agrega el comando list-volume y el menú desplegable de volumen a la configuración de Amazon EC2Launch. • Agrega el comando get-agent-config para imprimir el archivo agent-config.yml en formato yaml o json. • Borra la contraseña estática si no se detecta ninguna clave pública.	6 de octubre de 2020
2.0.124	• Agrega una opción para mostrar la versión del sistema operativo en el fondo de pantalla. • Inicializa los volúmenes de EBS cifrados. • Agrega rutas para VPC sin nombre DNS local.	10 de septiembre de 2020
2.0.104	• Crea una lista de búsqueda de sufijos DNS si no existe. • Omite la Hibernación si no se solicita.	12 de agosto de 2020
2.0.0	Versión inicial.	30 de junio de 2020

Historial de versiones de la herramienta de migración de EC2Launch v2

En la siguiente tabla, se describen las versiones publicadas de la herramienta de migración de EC2Launch v2.

Versión	Detalles	Fecha de la versión
1.0.396	• Actualice la herramienta de migración con la versión más actual del agente de EC2Launch v2: 2.0.1924.	11 de junio de 2024
1.0.394	• Actualice la herramienta de migración con la versión más actual del agente de EC2Launch v2: 2.0.1914.	6 de junio de 2024
1.0.384	• Actualice la herramienta de migración con la versión más actual del agente de EC2Launch v2: 2.0.1881.	8 de mayo de 2024
1.0.358	• Actualice la herramienta de migración con la última versión del agente de EC2launch v2: 2.0.1815.	8 de marzo de 2024
1.0.345	• Actualización de la herramienta de migración con la última versión del agente de EC2launch v2: 2.0.1739.	18 de enero de 2024
1.0.342	• Actualización de la herramienta de migración con la última versión del agente de EC2launch v2: 2.0.1702.	5 de enero de 2024
1.0.331	• Actualización de la herramienta de migración con la última versión del agente de EC2launch v2: 2.0.1643. • Corrección de un error que se produce al ejecutar `.Install.ps1 -DryRun .` • Solución de un problema que provocaba que la configuración de la contraseña se configurara incorrectamente como `random` durante la migración desde EC2Config.	3 de noviembre de 2023

Versión	Detalles	Fecha de la versión
	• Corrección de un error que se producía si `setWallpaper` se configuraba como `False` durante la migración desde EC2launch.	
1.0.303	Actualice la herramienta de migración con la última versión del agente de EC2launch v2: 2.0.1580.	14 de septiembre de 2023
1.0.286	Actualice la herramienta de migración con la última versión del agente de EC2launch v2: 2.0.1521.	14 de julio de 2023
1.0.272	Actualice la herramienta de migración con la última versión del agente de EC2launch v2: 2.0.1303.	3 de mayo de 2023
1.0.262	Actualice la herramienta de migración con la última versión del agente de EC2launch v2: 2.0.1245.	9 de marzo de 2023
1.0.241	Incrementa el número de versión del agente de EC2Launch v2 a 2.0.1011.	7 de diciembre de 2022
1.0.218	• Valida el valor de región recuperado de los metadatos de la instancia. • Corrige el error de migración en los paquetes de idioma. • Incrementa el número de versión del agente de EC2Launch v2 a 2.0.863.	3 de septiembre de 2022
1.0.162	• Traslada la lógica para eliminar agentes heredados al archivo MSI de EC2Launch v2. • Incrementa el número de versión del agente de EC2Launch v2 a 2.0.698.	18 de marzo de 2022
1.0.136	Incrementa el número de versión del agente de EC2Launch v2 a 2.0.651.	13 de octubre de 2021

Versión	Detalles	Fecha de la versión
1.0.130	Incrementa el número de versión del agente de EC2Launch v2 a 2.0.548.	5 de agosto de 2021
1.0.113	Utiliza IMDSv2 en lugar de IMDSv1.	4 de junio de 2021
1.0.101	Incrementa el número de versión del agente de EC2Launch v2 a 2.0.285.	12 de marzo de 2021
1.0.86	Incrementa el número de versión del agente de EC2Launch v2 a 2.0.207.	3 de febrero de 2021
1.0.76	Incrementa el número de versión del agente de EC2Launch v2 a 2.0.160.	4 de diciembre de 2020
1.0.69	Incrementa el número de versión del agente de EC2Launch v2 a 2.0.153.	5 de noviembre de 2020
1.0.65	Incrementa el número de versión del agente de EC2Launch v2 a 2.0.146.	9 de octubre de 2020
1.0.60	Incrementa el número de versión del agente de EC2Launch v2 a 2.0.124.	10 de septiembre de 2020
1.0.54	• Instala EC2Launch v2 si no hay agentes instalados. • Incrementa el número de versión del agente de EC2Launch v2 a 2.0.104. • Desacopla SSM Agent.	12 de agosto de 2020

Versión	Detalles	Fecha de la versión
1.0.50	Elimina la dependencia de NuGet.	10 de agosto de 2020
1.0.0	Versión inicial.	30 de junio de 2020

Configurar una instancia de Windows utilizando EC2Launch

EC2Launch es un conjunto de scripts de Windows PowerShell que sustituyó al servicio EC2Config en las AMI de Windows Server 2016 y 2019. Muchas de estas AMI siguen disponibles. El último servicio de inicialización para todas las versiones compatibles de Windows Server es EC2Launch v2, que reemplaza tanto EC2Config como EC2Launch. Para obtener más información, consulte Configurar una instancia de Windows mediante EC2Launch v2.

> **Note**
>
> Para utilizar EC2Launch con IMDSv2, la versión debe ser la 1.3.2002730 o posterior.

Contenido

Tareas de EC2Launch

EC2Launch realiza las siguientes tareas de manera predeterminada cuando la instancia se inicia por primera vez:

- Configura un fondo de pantalla nuevo en el que se representa información sobre la instancia.
- Establece el nombre del equipo en la dirección IPv4 privada de la instancia.
- Envía información sobre la instancia a la consola de Amazon EC2.
- Envía la huella digital del certificado RDP a la consola de EC2.
- Establece una contraseña aleatoria para la cuenta de administrador.
- Añade sufijos de DNS.
- Amplía dinámicamente la partición del sistema operativo para incluir cualquier espacio sin particionar.
- Ejecuta datos de usuario (si se especifica). Para obtener más información acerca de cómo especificar datos de usuario, consulte Trabajar con los datos de usuario de la instancia.
- Establece rutas estáticas persistentes para alcanzar el servicio de metadatos y los servidores AWS KMS.

> **Important**
>
> Si se crea una AMI personalizada desde esta instancia, estas rutas se capturan como parte de la configuración del SO y todas las instancias nuevas iniciadas desde la AMI conservarán las mismas rutas, independientemente de la ubicación de la subred. Para actualizar las rutas, consulte Actualice las rutas de metadatos/KMS para Server 2016 y versiones posteriores al iniciar una AMI personalizada..

La siguientes tareas ayudan a mantener la compatibilidad con versiones anteriores del servicio EC2Config. También puede configurar EC2Launch para que realice estas tareas al inicio:

- Inicializar volúmenes de EBS secundarios.
- Enviar registros de eventos de Windows a los registros de la consola de EC2.
- Enviar el mensaje Windows is ready to use (Windows está listo para utilizarse) a la consola de EC2.

Para obtener más información acerca de Windows Server 2019, consulte Comparación de características entre las versiones de Windows Server en Microsoft.com.

Telemetría

La telemetría es información adicional que ayuda a AWS a comprender mejor sus requisitos, diagnosticar problemas y ofrecer recursos para mejorar su experiencia con los servicios de AWS.

La versión `1.3.2003498` de EC2Launch y posteriores recopilan telemetría, como métricas de uso y errores. Estos datos se recopilan de la instancia de Amazon EC2 en la que se ejecuta EC2Launch. Esto incluye todas las AMI de Windows que son propiedad de AWS.

EC2Launch recopila los siguientes tipos de telemetría:

- Información de uso: comandos del agente, método de instalación y frecuencia de ejecución programada.
- Errores e información de diagnóstico: instalación del agente y ejecución de códigos de error.

Ejemplos de datos recopilados:

```
2021/07/15 21:44:12Z: EC2LaunchTelemetry: IsAgentScheduledPerBoot=true
2021/07/15 21:44:12Z: EC2LaunchTelemetry: IsUserDataScheduledPerBoot=true
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentCommandCode=1
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentCommandErrorCode=5
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentInstallCode=2
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentInstallErrorCode=0
```

La telemetría se encuentra habilitada de forma predeterminada. Puede desactivar la recopilación de telemetría en cualquier momento. Si la telemetría se encuentra habilitada, EC2Launch envía datos de telemetría sin notificaciones adicionales de los clientes.

Se recopila la elección de habilitar o desactivar la telemetría.

Puede optar por activar o desactivar la recolección de telemetría. Se recopila la opción elegida para participar o no de la telemetría a fin de garantizar que se cumpla con la opción de telemetría seleccionada.

Visibilidad de telemetría

Cuando la telemetría se encuentra habilitada, aparece en el resultado de la consola de Amazon EC2 de la siguiente manera:

```
2021/07/15 21:44:12Z: Telemetry: <Data>
```

Desactivar la telemetría en una instancia

Para desactivar la telemetría al establecer una variable de entorno de sistema, ejecute el siguiente comando como administrador:

```
setx /M EC2LAUNCH_TELEMETRY 0
```

Para desactivar la telemetría durante la instalación, ejecute `install.ps1` de la siguiente manera:

```
. .\install.ps1 -EnableTelemetry:$false
```

Instalar la versión más reciente de EC2Launch

Utilice el siguiente procedimiento para descargar e instalar la versión más reciente de EC2Launch en sus instancias.

Para descargar e instalar la versión más reciente de EC2Launch

1. Si ya ha instalado y configurado EC2Launch en una instancia, realice una copia de seguridad del archivo de configuración de EC2Launch. Durante el proceso de instalación, no se conservan los cambios realizados en este archivo. De forma predeterminada, el archivo se ubica en el directorio `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.
2. Descargue EC2-Windows-Launch.zip en un directorio de la instancia.
3. Descargue install.ps1 en el mismo directorio en que ha descargado `EC2-Windows-Launch.zip`.
4. Ejecute `install.ps1`
5. Si ha realizado una copia de seguridad del archivo de configuración de EC2Launch, cópielo en el directorio `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.

Para descargar e instalar la versión más reciente de EC2Launch v2 utilizando PowerShell

Si ya ha instalado y configurado EC2Launch en una instancia, realice una copia de seguridad del archivo de configuración de EC2Launch. Durante el proceso de instalación, no se conservan los cambios realizados en este archivo. De forma predeterminada, el archivo se ubica en el directorio `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.

Para instalar la versión más reciente de EC2Launch mediante PowerShell, ejecute los siguientes comandos desde una ventana de PowerShell

```
mkdir $env:USERPROFILE\Desktop\EC2Launch
$Url = "https://s3.amazonaws.com/ec2-downloads-windows/EC2Launch/latest/EC2-Windows-
Launch.zip"
$DownloadZipFile = "$env:USERPROFILE\Desktop\EC2Launch\" + $(Split-Path -Path $Url -
Leaf)
Invoke-WebRequest -Uri $Url -OutFile $DownloadZipFile
$Url = "https://s3.amazonaws.com/ec2-downloads-windows/EC2Launch/latest/install.ps1"
$DownloadZipFile = "$env:USERPROFILE\Desktop\EC2Launch\" + $(Split-Path -Path $Url -
Leaf)
Invoke-WebRequest -Uri $Url -OutFile $DownloadZipFile
& $env:USERPROFILE\Desktop\EC2Launch\install.ps1
```

> **Note**
>
> Si recibe un error al descargar el archivo y está usando Windows Server 2016, es posible que sea necesario habilitar TLS 1.2 para su terminal PowerShell. Puede habilitar TLS 1.2 para la sesión actual de PowerShell con el siguiente comando y luego volver a intentarlo:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
> ```

Verifique la instalación comprobando `C:\ProgramData\Amazon\EC2-Windows\Launch`.

Verificación de la versión de EC2Launch

Use el siguiente comando de Windows PowerShell para verificar la versión instalada de EC2Launch.

```
PS C:\> Test-ModuleManifest -Path "C:\ProgramData\Amazon\EC2-Windows\Launch\Module
\Ec2Launch.psd1" | Select Version
```

Estructura de directorios de EC2Launch

EC2Launch se instala de manera predeterminada en las AMI para Windows Server 2016 y versiones posteriores, en el directorio raíz `C:\ProgramData\Amazon\EC2-Windows\Launch`.

> **Note**
>
> De manera predeterminada, Windows oculta los archivos y las carpetas en `C:\ProgramData`. Para ver los directorios y los archivos de EC2Launch, debe escribir la ruta

de acceso en el Explorador de Windows o cambiar las propiedades de carpeta para ver los archivos y carpetas ocultos.

El directorio `Launch` contiene los subdirectorios siguientes.

- `Scripts` — contiene los scripts de PowerShell que conforman EC2Launch.
- `Module` — contiene el módulo para crear scripts relacionados con Amazon EC2.
- `Config` — contiene archivos de configuración de scripts que se pueden personalizar.
- `Sysprep` — contiene los recursos de Sysprep.
- `Settings` — contiene una aplicación para la interfaz gráfica de usuario de Sysprep.
- `Library`: contiene bibliotecas de uso compartido para los agentes de inicialización de EC2.
- `Logs` — contiene los archivos de registro generados por los scripts.

Versión **`1.3.2004592`** y posteriores de EC2Launch

Los usuarios del grupo `Administrators` tienen permisos `Full control` para acceder a todos los directorios de EC2launch. Los usuarios que no están en el grupo Administradores tienen permisos `Read & execute` para acceder a todos los directorios de EC2launch excepto `C:\ProgramData\Amazon\EC2-Windows\Launch\Module\Config`. El directorio `Config` está restringido a los usuarios que son miembros del grupo `Administrators`.

Versión **`1.3.2004491`** y anteriores de EC2Launch

Todos los directorios EC2Launch heredan sus permisos de `C:\ProgramData`, excepto `C:\ProgramData\Amazon\EC2-Windows\Launch\Module\Scripts`. Esta carpeta hereda todos los permisos iniciales de `C:\ProgramData` cuando se crea, pero quita el acceso de los usuarios normales a `CreateFiles` en el directorio.

Configurar EC2Launch

Después de inicializar por primera vez la instancia, puede volver a configurar EC2Launch para que se vuelva a ejecutar y realice diferentes tareas al inicio.

Tareas

- Configurar tareas de inicialización
- Programar EC2Launch para que se ejecute en cada arranque

- Inicialización de unidades y mapeos de letras de unidad
- Envío de registros de eventos de Windows a la consola de EC2
- Envío del mensaje Windows Is Ready después de un arranque correcto

Configurar tareas de inicialización

Especifique las opciones en el archivo `LaunchConfig.json` para habilitar o deshabilitar las siguientes tareas de inicialización:

- Establezca el nombre del equipo en la dirección IPv4 privada de la instancia.
- Configura el monitor para que permanezca siempre encendido.
- Configurar un fondo de pantalla nuevo.
- Añadir una lista de sufijos de DNS.

> **Note**
>
> Esto agrega una búsqueda de sufijos de DNS para el siguiente dominio y configura otros sufijos estándar. Para obtener más información acerca de cómo los agentes de inicialización configuran los sufijos de DNS, consulte Configuración del sufijo de DNS para los agentes de inicialización de Windows.
>
> ```
> region.ec2-utilities.amazonaws.com
> ```

- Ampliar el tamaño del volumen de arranque.
- Establecer la contraseña del administrador.

Para configurar los ajustes de inicialización

1. En la instancia que se va a configurar, abra el archivo siguiente en un editor de texto: `C:\ProgramData\Amazon\EC2-Windows\Launch\Config\LaunchConfig.json`.
2. Actualice la configuración siguiente como sea necesario y guarde los cambios. Proporcione una contraseña en `adminPassword` solo si `adminPasswordtype` es `Specify`.

```
{
 "setComputerName": false,
 "setMonitorAlwaysOn": true,
```

```
 "setWallpaper": true,
 "addDnsSuffixList": true,
 "extendBootVolumeSize": true,
 "handleUserData": true,
 "adminPasswordType": "Random | Specify | DoNothing",
 "adminPassword": "password that adheres to your security policy (optional)"
}
```

Los tipos de contraseñas se definen de la siguiente manera:

`Random`

EC2Launch genera una contraseña y la cifra usando la clave del usuario. El sistema deshabilita esta configuración tras la inicialización de la instancia para que esta contraseña persista si la instancia se reinicia o si se detiene y se inicia.

`Specify`

EC2Launch usa la contraseña que ha especificado en `adminPassword`. Si la contraseña no cumple los requisitos del sistema, EC2Launch genera una contraseña aleatoria en su lugar. La contraseña se almacena en `LaunchConfig.json` como texto sin cifrar y se elimina cuando Sysprep define la contraseña del administrador. EC2Launch cifra la contraseña usando la clave del usuario.

`DoNothing`

EC2Launch usa la contraseña que ha especificado en el archivo `unattend.xml`. Si no especifica una contraseña en el archivo `unattend.xml`, la cuenta del administrador se deshabilitará.

3. En Windows PowerShell, ejecute el siguiente comando para programar el script para que se ejecute como una tarea programada de Windows. El script se ejecuta una vez durante el siguiente arranque y, luego, deshabilita estas tareas para que no vuelvan a ejecutarse.

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
Schedule
```

Programar EC2Launch para que se ejecute en cada arranque

Puede programar EC2Launch para que se ejecute en cada arranque en lugar de solo en el arranque inicial.

Para permitir que EC2Launch se ejecute en cada arranque:

1. Abra Windows PowerShell y ejecute el comando siguiente:

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
SchedulePerBoot
```

2. O lance el ejecutable con el siguiente comando:

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Settings\Ec2LaunchSettings.exe
```

   A continuación, seleccione `Run EC2Launch on every boot`. Puede especificar que su instancia de EC2 `Shutdown without Sysprep` o `Shutdown with Sysprep`.

> **Note**
>
> Si permite que EC2Launch se ejecute en cada arranque, sucederá lo siguiente la próxima vez que lo haga:
>
> - Si `AdminPasswordType` aún está establecida como `Random`, EC2Launch generará una nueva contraseña en el siguiente arranque. Luego de ese arranque, `AdminPasswordType` se establece automáticamente como `DoNothing` para impedir que EC2Launch genere nuevas contraseñas en los siguientes arranques. Para impedir que EC2Launch genere una nueva contraseña en el primer arranque, establezca manualmente `AdminPasswordType` en `DoNothing` antes de reiniciar.
> - `HandleUserData` se volverá a establecer en `false` a menos que los datos de usuarios tengan `persist` establecido como `true`. Para obtener más información, consulte the section called “Scripts de datos de usuario”.

Inicialización de unidades y mapeos de letras de unidad

Especifique opciones en el archivo `DriveLetterMappingConfig.json` para mapear letras de unidades a volúmenes en la instancia de EC2. El script inicializa las unidades que aún no se han inicializado y particionado. Para obtener más información sobre cómo obtener detalles de volúmenes en Windows, consulte Get-Volume en la documentación de Microsoft.

Para mapear las letras de unidad con los volúmenes

1. Abra el archivo `C:\ProgramData\Amazon\EC2-Windows\Launch\Config\DriveLetterMappingConfig.json` en un editor de texto.
2. Especifique la siguiente configuración del volumen y guarde los cambios:

```
{
 "driveLetterMapping": [
  {
   "volumeName": "sample volume",
   "driveLetter": "H"
  }
 ]
}
```

3. Abra Windows PowerShell y utilice el siguiente comando para ejecutar el script de EC2Launch que inicializa los discos:

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1
```

   Para inicializar los discos cada vez que se arranca la instancia, añada la marca `-Schedule` de la siguiente manera:

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1 -
Schedule
```

Envío de registros de eventos de Windows a la consola de EC2

Especifique opciones en el archivo `EventLogConfig.json` para enviar registros de eventos de Windows a los registros de la consola de EC2.

Para configurar ajustes para enviar registros de eventos de Windows

1. En la instancia, abra el archivo `C:\ProgramData\Amazon\EC2-Windows\Launch\Config\EventLogConfig.json` en un editor de texto.
2. Configure los siguientes ajustes del registro y guarde los cambios:

```
{
 "events": [
```

```
  {
   "logName": "System",
   "source": "An event source (optional)",
   "level": "Error | Warning | Information",
   "numEntries": 3
  }
 ]
}
```

3. En Windows PowerShell, ejecute el siguiente comando para que el sistema programe el script para que se ejecute como una tarea programada de Windows cada vez que se arranca la instancia.

   ```
   PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\SendEventLogs.ps1 -
   Schedule
   ```

   Los registros pueden tardar tres minutos o más en aparecer en los registros de la consola de EC2.

Envío del mensaje Windows Is Ready después de un arranque correcto

El servicio EC2Config envía el mensaje “Windows is ready” a la consola de EC2 después de cada arranque. EC2Launch solo envía este mensaje la primera vez que se arranca. Para que sea compatible con versiones anteriores del servicio EC2Config, puede programar EC2Launch para que envíe este mensaje después de cada arranque. En la instancia, abra Windows PowerShell y ejecute el comando siguiente. El sistema programa el script para que se ejecute como una tarea programada de Windows.

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\SendWindowsIsReady.ps1 -
Schedule
```

Historial de versiones de EC2Launch

Desde Windows Server 2016, las AMI de Windows incluyen un conjunto de scripts de Windows PowerShell que se denomina EC2Launch. EC2Launch realiza ciertas tareas durante el arranque inicial de la instancia. Para obtener más información sobre las versiones de EC2Launch incluidas en las AMI de Windows de AWS, consulte Historial de versiones de AMI de Windows de AWS.

Para descargar e instalar la versión más reciente de EC2Launch, consulte Instalar la versión más reciente de EC2Launch.

En la siguiente tabla se describen las versiones de EC2Launch publicadas. Tenga en cuenta que el formato de versión cambió después de la versión 1.3.610.

Versión	Detalles	Fecha de la versión
1.3.2004891	• Se solucionó un problema en el que `HandleUserData` no estaba configurado como `false`, como se esperaba. • Se agregó una opción de contraseña `Encrypted` a `LaunchConfig.json` . • Se modificó el comportamiento de la `Settings UI` para cifrar la contraseña especificada por el usuario de forma predeterminada. • Se agregó `SetAdminPasswordConfig.ps1` para convertir la opción de `Specify` contraseña en la opción de contraseña `Encrypted` en el archivo de configuración del agente.	31 de mayo de 2024
1.3.2004617	• Se corrigió un error al configurar el fondo de pantalla.	15 de enero de 2024
1.3.2004592	• Se actualizaron los permisos de acceso establecidos por install.ps1 para `%ProgramData%\Amazon\EC2-Windows\Launch` . • Se restringió el acceso a las carpetas y archivos de EC2Launch para lectura y ejecución únicamente para las cuentas de usuario estándar. • Se modificó el agente para dejar de esperar a que el servicio de metadatos de instancias (IMDS) se inicie si IMDS no está habilitado para la instancia. •	2 de enero de 2024

Versión	Detalles	Fecha de la versión
	Se agregó un tiempo de espera de cinco minutos para que se inicialice el IMDS. • Se cambió el agente para que escriba la telemetría en el registro de la consola de la instancia antes del mensaje `Windows is Ready` y no después. • Se agregó compatibilidad con fondos de escritorio para varios tipos de instancia nuevos. Para obtener más información sobre los permisos de acceso y los permisos de las cuentas de usuario de los directorios de EC2launch, consulte the section called “Estructura de directorios de EC2Launch”.	
1.3.2004491	• Se agregó telemetría para supervisar el uso de la opción Especificar contraseña de administrador.	9 de noviembre de 2023
1.3.2004462	• Se agregó un elemento flush después de cada escritura en la consola serie.	18 de octubre de 2023

Versión	Detalles	Fecha de la versión
1.3.2004438	• Limite la devolución de nombres de dominio en función de la entrada de registro: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters\DomainNameDevolutionLevel` . • Permisos de `UserdataExecution.log` limitados solo a `Administrators` . • Se agregaron mensajes de error en el registro de eventos de Windows cuando se produce un error en la inicialización del registro.	4 de octubre de 2023
1.3.2004256	• Se ha agregado un valor `EnableSCSIPersistentReservations` de la consola. • Se agregó la capacidad de reintento para Get-ConsolePort.	7 de julio de 2023
1.3.2004052	• Se ha solucionado un error que se producía cuando no se especificaba ninguna clave de SSH al iniciar la instancia. • Se ha actualizado para volver a intentar iniciar el servicio AmazonSSMAgent para Windows en caso de error. • Se ha actualizado para que no funcione SysprepInstance.ps1 si BeforeSysprep.cmd da error con un código de salida distinto de cero.	8 de marzo de 2023
1.3.2003975	• Se solucionó un problema que afectaba a las compilaciones de AMI de Packer en el que `SysprepInstance.ps1` devolvía un `$LastErrorCode` de 1.	24 de diciembre de 2022

Versión	Detalles	Fecha de la versión
1.3.2003961	• Se solucionó un problema que hacía que las contraseñas de administrador especificadas explícitamente se sobrescribieran con una contraseña aleatoria en las instancias de inicio rápido. • Se solucionó un problema que hacía que el agente SSM no se iniciara en tipos de instancias más pequeños. • Se solucionó un problema por el que el registro de la consola de instancias contenía `RDPCERTIFICATE-THUMBPRINT: 0000000000000000000000` en lugar de un valor de huella digital de certificado de RDP válido.	6 de diciembre de 2022
1.3.2003923	• Corrige la lógica para encontrar el adaptador de red cuando PnPDeviceID está vacío.	9 de noviembre de 2022
1.3.2003919	• Se actualizó Get-ConsolePort para usar la información del segmento PCI. • Se solucionó un problema por el que se podía seleccionar un adaptador de red incorrecto tras reiniciar. • Se corrigió la lógica de tiempo de espera de start-SSM-Agent. • Se corrigió la compatibilidad con versiones anteriores del alias de la función Send-AdminCredentials.	8 de noviembre de 2022
1.3.2003857	• Prioriza los adaptadores con una puerta de enlace predeterminada cuando se selecciona el adaptador de red principal. • Cifrado de contraseña extendido en memoria.	3 de octubre de 2022

Versión	Detalles	Fecha de la versión
1.3.2003824	• Se corrigió un error durante `setComputerName` . • Se agregó una lógica para omitir la activación de Windows cuando se detecta un código de facturación BYOL. • Se agregó cifrado de contraseña en memoria. • Se corrigió un error durante la inicialización del volumen en `m6id.4xlarge` .	30 de agosto de 2022
1.3.2003691	• Se actualizó la lógica de espera de IMDS para realizar solo solicitudes IMDSv2. • Se ha corregido un error que afectaba a la instalación de eGPU.	21 de junio de 2022
1.3.2003639	• Se agregó la lógica de espera del adaptador de red para evitar su uso antes de la inicialización. • Se han corregido problemas de menor importancia.	10 de mayo de 2022
1.3.2003498	• Se agregó telemetría. • Se agregó acceso directo a la interfaz de usuario de la configuración. • Scripts de PowerShell formateados. • Se corrigió el problema con un apagado que ocurre antes de que se complete BeforResysprep.cmd.	31 de enero de 2022
1.3.2003411	Se ha cambiado la lógica de generación de contraseñas para excluir contraseñas de baja complejidad.	04 de agosto de 2021
1.3.2003364	Se actualizó Install-EgpuManager con soporte para IMDSv2.	7 de junio de 2021

Versión	Detalles	Fecha de la versión
1.3.2003312	• Se agregaron líneas de registro antes y después la configuración de `setMonitorAlwaysOn` . • Se ha añadido versión del paquete de Nitro Enclaves de AWS al registro de la consola.	4 de mayo de 2021
1.3.2003284	Modelo de permisos mejorado mediante la actualización de la ubicación para almacenar datos de usuario en `LocalAppData` .	23 de marzo de 2021
1.3.2003236	• Método actualizado para establecer la contraseña de usuario en `Set-AdminAccount` y `Randomize-LocalAdminPassword` . • Se ha corregido`InitializeDisks` para comprobar si el disco está configurado para sólo lectura antes de configurarlo como de escritura.	11 de febrero de 2021
1.3.2003210	Corrección de localización de `install.ps1` .	7 de enero de 2021
1.3.2003205	Corrección de seguridad de `install.ps1` para actualizar los permisos en el directorio `%ProgramData%AmazonEC2-WindowsLaunchModuleScripts` .	28 de diciembre de 2020
1.3.2003189	Añadido `w32tm resync` después de añadir rutas.	4 de diciembre de 2020
1.3.2003155	Información actualizada del tipo de instancia.	25 de agosto de 2020
1.3.2003150	Se ha agregado `OsCurrentBuild` y `OsReleaseId` al resultado de la consola.	22 de abril de 2020

Versión	Detalles	Fecha de la versión
1.3.2003040	Se ha corregido la lógica alternativa 1 de la versión IMDS.	7 de abril de 2020
1.3.2002730	Se ha agregado compatibilidad para IMDS V2.	3 de marzo de 2020
1.3.2002240	Se han corregido problemas de menor importancia.	31 de octubre de 2019
1.3.2001660	Se ha corregido el problema de inicio de sesión automático para usuarios sin contraseña después de ejecutar por primera vez Sysprep.	2 de julio de 2019
1.3.2001360	Se han corregido problemas de menor importancia.	27 de marzo de 2019
1.3.2001220	Todos los scripts de PowerShell firmados.	28 de febrero de 2019
1.3.2001200	Se ha solucionado un problema con InitializeDisks.ps1 donde al ejecutar el script en un nodo de un clúster de conmutación por error de Windows Server se formateaban las unidades de los nodos remotos cuyas letras coincidían con la letra de la unidad local.	27 de febrero de 2019
1.3.2001160	Se ha solucionado un problema con el fondo de pantalla en Windows 2019.	22 de febrero de 2019
1.3.2001040	• Se ha añadido un complemento para definir que el monitor no se apague nunca para corregir problemas de ACPI. • La versión y edición de SQL Server se escriben en la consola.	21 de enero de 2019
1.3.2000930	Corrección para añadir rutas a metadatos en las ENI habilitadas para ipv6.	2 de enero de 2019

Versión	Detalles	Fecha de la versión
1.3.2000760	• Configuración predeterminada añadida para la configuración de RSS y Recibir colas para dispositivos ENA. • Hibernación deshabilitada durante Sysprep.	5 de diciembre de 2018
1.3.2000630	• Ruta 169.254.169.253/32 añadida para el servidor DNS. • Filtro añadido para la configuración Usuario administrativo. • Mejoras en la hibernación de instancias. • Opción añadida para programar EC2Launch para que se ejecute en cada arranque.	9 de noviembre de 2018
1.3.2000430.0	• Se ha añadido la ruta 169.254.169.123/32 al servicio de hora AMZN. • Se ha añadido la ruta 169.254.169.249/32 al servicio de licencias GRID. • Se ha añadido un tiempo de espera de 25 segundos al intentar iniciar Systems Manager.	19 de septiembre de 2018
1.3.200039.0	• Se ha corregido la asignación incorrecta de letras de unidad para los volúmenes NVME de EBS. • Se han añadido funciones de registro adicional para las versiones de los controladores NVME.	15 de agosto de 2018
1.3.2000080	Se han corregido problemas de menor importancia.	
1.3.610	Se ha corregido el problema del redireccionamiento de salidas y errores hacia archivos desde los datos del usuario.	
1.3.590	• Se han añadido al fondo de pantalla los tipos de instancias que faltaban. • Se ha corregido el problema con el mapeo de las letras de unidades y la instalación de los discos.	

Versión	Detalles	Fecha de la versión
1.3.580	• Se ha corregido `Get-Metadata` para que use la configuración predeterminada del sistema en las solicitudes web. • Se ha añadido un caso especial para NVMe en la inicialización de los discos. • Se han corregido problemas de menor importancia.	
1.3.550	Se ha añadido la opción `-NoShutdown` para habilitar la ejecución de Sysprep sin apagado.	
1.3.540	Se han corregido problemas de menor importancia.	
1.3.530	Se han corregido problemas de menor importancia.	
1.3.521	Se han corregido problemas de menor importancia.	
1.3.0	• Se ha corregido un problema en la longitud hexadecimal en los cambios de nombre de los equipos. • Se ha corregido un posible bucle de reinicio en los cambios de nombre de los equipos. • Se ha corregido un problema en la configuración del fondo de pantalla.	
1.2.0	• Actualización para ver la información sobre el sistema operativo instalado (SO) en el registro del sistema de EC2. • Actualización para ver la versión de EC2Launch y SSM Agent en el registro del sistema de EC2. • Se han corregido problemas de menor importancia.	

Versión	Detalles	Fecha de la versión
1.1.2	• Actualización para ver la información de los controladores de ENA en el registro del sistema de EC2. • Actualización para excluir Hyper-V de la lógica del filtro de NIC primario. • Se ha agregado el servidor y el puerto de AWS KMS a la clave del registro para la activación de KMS. • Se ha mejorado la configuración del fondo de pantalla para varios usuarios. • Actualización para borrar rutas desde el almacén persistente. • Actualización para eliminar la z de la zona de disponibilidad en la lista de sufijos de DNS. • Actualización para solucionar un problema con la etiqueta <runAsLocalSystem> en los datos de usuario.	
1.1.1	Versión inicial.	

Configuración de una instancia de Windows mediante el servicio EC2Config (heredado)

> **Note**
>
> La documentación de EC2Config se proporciona únicamente como referencia histórica. Microsoft ya no admite las versiones del sistema operativo en las que se ejecuta. Recomendamos encarecidamente que actualice al servicio de lanzamiento más reciente. El último servicio de inicialización para Windows Server 2022 es EC2Launch v2, que reemplaza a EC2Config y EC2Launch.

Las AMI de Windows Server anteriores a Windows Server 2016 incluyen un servicio opcional llamado servicio EC2Config (`EC2Config.exe`). EC2Config se inicia cuando la instancia arranca y realiza tareas durante el inicio, así como cada vez que detiene o inicia la instancia. EC2Config también puede realizar tareas previa petición. Algunas de estas tareas se activan automáticamente, mientras que otras se deben activar manualmente. Aunque este servicio es opcional, proporciona acceso a funciones avanzadas que, de otro modo, no estarían disponibles. Este servicio se ejecuta en la cuenta LocalSystem.

> **Note**
>
> EC2Launch sustituyó a EC2Config en las AMI de Windows Server 2016 y 2019. Para obtener más información, consulte Configurar una instancia de Windows utilizando EC2Launch. El último servicio de inicialización para todas las versiones compatibles de Windows Server es EC2Launch v2, que reemplaza tanto EC2Config como EC2Launch.

EC2Config utiliza archivos de configuración para controlar su operación. Puede actualizar esta configuración mediante una herramienta gráfica o editando los archivos XML directamente. Los archivos binarios y los archivos adicionales del servicio se encuentran en el directorio `%ProgramFiles%\Amazon\EC2ConfigService`.

Contenido

Tareas de EC2Config

EC2Config ejecuta tareas de arranque inicial cuando la instancia se inicia por primera vez y, a continuación, las desactiva. Para volver a ejecutar estas tareas, debe habilitarlas de forma explícita antes de cerrar la instancia o ejecutando Sysprep manualmente. Estas tareas son las siguientes:

- Establecer una contraseña cifrada aleatoria para la cuenta de administrador.
- Generar e instalar el certificado host utilizado para la conexión de escritorio remoto.
- Ampliar dinámicamente la partición del sistema operativo para incluir cualquier espacio sin particionar.
- Ejecutar los datos de usuario especificados (y Cloud-Init si está instalado). Para obtener más información acerca de cómo especificar datos de usuario, consulte Trabajar con los datos de usuario de la instancia.

EC2Config realiza las siguientes tareas cada vez que se inicia la instancia:

- Cambio del nombre de host para que coincida la dirección IP privada en notación hexadecimal (está tarea está deshabilitada de forma predeterminada y debe habilitarse para que se ejecute al iniciarse la instancia).
- Configuración del servidor de administración de claves (AWS KMS), comprobación del estado de activación de Windows y activación de Windows según sea necesario.
- Montaje de todos los volúmenes de Amazon EBS, volúmenes de almacén de instancias y nombres de volúmenes de mapeo en letras de unidad.
- Escritura de entradas de registro de eventos en la consola para ayudar con la solución de problemas (está tarea está deshabilitada de forma predeterminada y debe habilitarse para que se ejecute al iniciarse la instancia).
- Escritura de la disponibilidad de Windows en la consola.
- Agregue una ruta personalizada al adaptador de red principal para habilitar las siguientes direcciones IP cuando se adjuntan una o varias NIC: `169.254.169.250`, `169.254.169.251` y `169.254.169.254`. Estas direcciones las utiliza la activación de Windows y cuando se obtiene acceso a los metadatos de la instancia.

> **Note**
>
> Si el sistema operativo Windows está configurado para utilizar IPv4, se pueden utilizar estas direcciones locales de enlace IPv4. Si el sistema operativo Windows tiene la pila de

protocolos de red IPv4 desactivada y usa IPv6 en su lugar, agregue `[fd00:ec2::240]` en lugar de `169.254.169.250` y `169.254.169.251`. A continuación, agregue `[fd00:ec2::254]` en lugar de `169.254.169.254`.

EC2Config realiza las siguientes tareas cada vez que un usuario inicia sesión:

- Muestra de la información de fondo de pantalla en el fondo del escritorio.

Cuando la instancia se está ejecutando, puede solicitar que EC2Config realice las siguientes tareas previa petición:

- Ejecución de Sysprep y cierre de la instancia para que pueda crear una AMI a partir de esta. Para obtener más información, consulte Creación de una AMI con Windows Sysprep.

Instalar la versión más reciente de EC2Config

De forma predeterminada, el servicio EC2Config está incluido en las AMI anteriores a Windows Server 2016. Al actualizar el servicio EC2Config, las nuevas AMI de Windows de AWS incluyen la versión más reciente del servicio. No obstante, necesitará actualizar sus propias AMI e instancias de Windows con la versión más reciente de EC2Config.

> **Note**
>
> EC2Launch sustituye a EC2Config en Windows Server 2016 y 2019. Para obtener más información, consulte Configurar una instancia de Windows utilizando EC2Launch. El último servicio de inicialización para todas las versiones compatibles de Windows Server es EC2Launch v2, que reemplaza tanto EC2Config como EC2Launch.

Para obtener información sobre cómo recibir notificaciones sobre actualizaciones de EC2Config, consulte Suscribirse a las notificaciones del servicio EC2Config. Para obtener información acerca de los cambios de cada versión, consulte Historial de versión de EC2Config.

Antes de empezar

- Verifique que tiene .NET framework 3.5 SP1 o superior.

- De forma predeterminada, el proceso de configuración sustituye los archivos de configuración existentes por otros con una configuración predeterminada durante la instalación y posteriormente reinicia el servicio EC2Config cuando se completa la instalación. Si ha cambiado la configuración del servicio EC2Config, copie el archivo `config.xml` del directorio `%Program Files%\Amazon\Ec2ConfigService\Settings`. Después de actualizar el servicio EC2Config, puede restaurar este archivo para conservar los cambios en la configuración.
- Si tiene una versión de EC2Config anterior a la versión 2.1.19 y va a instalar la versión 2.2.12 o una anterior, debe instalar primero la versión 2.1.19. Para instalar la versión 2.1.19, descargue EC2Install_2.1.19.zip, descomprima el archivo y, a continuación, ejecute `EC2Install.exe`.

> **Note**
>
> Si tiene una versión de EC2Config anterior a la versión 2.1.19 y va a instalar la versión 2.3.313 o una posterior, puede instalarla directamente sin instalar primero la versión 2.1.19.

Verificar la versión de EC2Config

Siga este procedimiento para verificar la versión de EC2Config que hay instalada en las instancias.

Para verificar la versión instalada de EC2Config

1. Lance una instancia desde la AMI y conéctese a ella.
2. En el panel de control, seleccione Programas y características.
3. En la lista de programas instalados, busque `Ec2ConfigService`. Su número de versión aparece en la columna Versión.

Actualización de EC2Config

Siga este procedimiento para descargar la versión más reciente de EC2Config e instalarla en las instancias.

Para descargar e instalar la versión más reciente de EC2Config

1. Descargue y descomprima el instalador de EC2Config.

2. Ejecute `EC2Install.exe`. Para obtener una lista completa de opciones, ejecute `EC2Install` con la opción `/?`. De forma predeterminada, el proceso de configuración muestra preguntas. Para ejecutar el comando sin este tipo de preguntas, utilice la opción `/quiet`.

   > **Important**
   >
   > Para mantener los ajustes personalizados del archivo `config.xml` que guardó, ejecute `EC2Install` con la opción `/norestart`, restaure la configuración y, a continuación, reinicie el servicio EC2Config manualmente.

3. Si ejecuta la versión 4.0 o posterior de EC2Config, debe reiniciar SSM Agent en la instancia desde el complemento de Microsoft Services.

   > **Note**
   >
   > La formación de la versión de EC2Config actualizada no aparecerá en el registro del sistema de la instancia ni en Trusted Advisor hasta que reinicie la instancia o la detenga y vuelva a iniciarla.

Para descargar e instalar la versión más reciente de EC2Config utilizando PowerShell

Para descargar, descomprimir e instalar la versión más reciente de EC2Config mediante PowerShell, ejecute los siguientes comandos desde una ventana de PowerShell

```
$Url = "https://s3.amazonaws.com/ec2-downloads-windows/EC2Config/EC2Install.zip"
$DownloadZipFile = "$env:USERPROFILE\Desktop\" + $(Split-Path -Path $Url -Leaf)
$ExtractPath = "$env:USERPROFILE\Desktop\"
Invoke-WebRequest -Uri $Url -OutFile $DownloadZipFile
$ExtractShell = New-Object -ComObject Shell.Application
$ExtractFiles = $ExtractShell.Namespace($DownloadZipFile).Items()
$ExtractShell.NameSpace($ExtractPath).CopyHere($ExtractFiles)
Start-Process $ExtractPath
Start-Process `
    -FilePath $env:USERPROFILE\Desktop\EC2Install.exe `
    -ArgumentList "/S"
```

> **Note**
>
> Si recibe un error al descargar el archivo y está usando Windows Server 2016 o una versión anterior, es posible que sea necesario habilitar TLS 1.2 para su terminal PowerShell. Puede habilitar TLS 1.2 para la sesión actual de PowerShell con el siguiente comando y luego volver a intentarlo:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
> ```

Verifique la instalación comprobando `C:\Program Files\Amazon\` para el directorio de `Ec2ConfigService`.

Detener, reiniciar, eliminar o desinstalar EC2Config

Puede administrar el servicio EC2Config igual que cualquier otro servicio.

Para aplicar la configuración actualizada a la instancia, puede detener y reiniciar el servicio. Si va a instalar EC2Config manualmente, primero debe detener el servicio.

Para detener el servicio EC2Config

1. Lance y conéctese a la instancia de Windows.
2. En el menú Inicio, seleccione Herramientas administrativas y, a continuación, haga clic en Servicios.
3. En la lista de servicios, haga clic con el botón derecho en EC2Config y seleccione Detener.

Para reiniciar el servicio EC2Config

1. Lance y conéctese a la instancia de Windows.
2. En el menú Inicio, seleccione Herramientas administrativas y, a continuación, haga clic en Servicios.
3. En la lista de servicios, haga clic con el botón derecho en EC2Config y seleccione Reiniciar.

Si no necesita actualizar las opciones de configuración, crear su propia AMI o utilizar AWS Systems Manager, puede eliminar y desinstalar el servicio. Si elimina un servicio, se eliminará su subclave de

registro. Si desinstala un servicio, se eliminarán los archivos, la subclave de registro y cualquier atajo del servicio.

Para eliminar el servicio EC2Config

1. Inicie una ventana del símbolo del sistema.
2. Ejecute el comando siguiente:

```
sc delete ec2config
```

Para desinstalar EC2Config

1. Lance y conéctese a la instancia de Windows.
2. En el menú Inicio, haga clic en Panel de control.
3. Haga doble clic en Programas y características.
4. En la lista de programas, seleccione EC2ConfigService y haga clic en Desinstalar.

EC2Config y AWS Systems Manager

El servicio EC2Config procesa las solicitudes de Systems Manager de las instancias creadas desde AMI para versiones de Windows Server anteriores a Windows Server 2016 publicadas con anterioridad a noviembre de 2016.

Las instancias creadas desde AMI para versiones de Windows Server anteriores a Windows Server 2016 publicadas con posterioridad a noviembre de 2016 incluyen el servicio EC2Config y el SSM Agent. EC2Config realiza todas las tareas descritas anteriormente y SSM Agent procesa las solicitudes para las características de Systems Manager como Run Command y State Manager.

Puede usar Run Command para actualizar las instancias existentes para que utilicen la versión más reciente del servicio EC2Config y de SSM Agent. Para obtener más información, consulte Actualizar el SSM Agent mediante Run Command en la Guía del usuario de AWS Systems Manager.

EC2Config y Sysprep

El servicio EC2Config ejecuta Sysprep, una herramienta de Microsoft que le permite crear una AMI de Windows personalizada que se puede reutilizar. Cuando EC2Config llama a Sysprep, utiliza los archivos de `%ProgramFiles%\Amazon\EC2ConfigService\Settings` para determinar qué

operaciones realizar. Puede editar estos archivos indirectamente desde el cuadro de diálogo EC2 Service Properties (Propiedades del servicio de EC2) o bien si utiliza directamente un editor de XML o de texto. Sin embargo, hay algunas opciones de configuración avanzada que no están disponibles en el cuadro de diálogo Ec2 Service Properties (Propiedades del servicio de EC2), por lo que debe editar dichas entradas directamente.

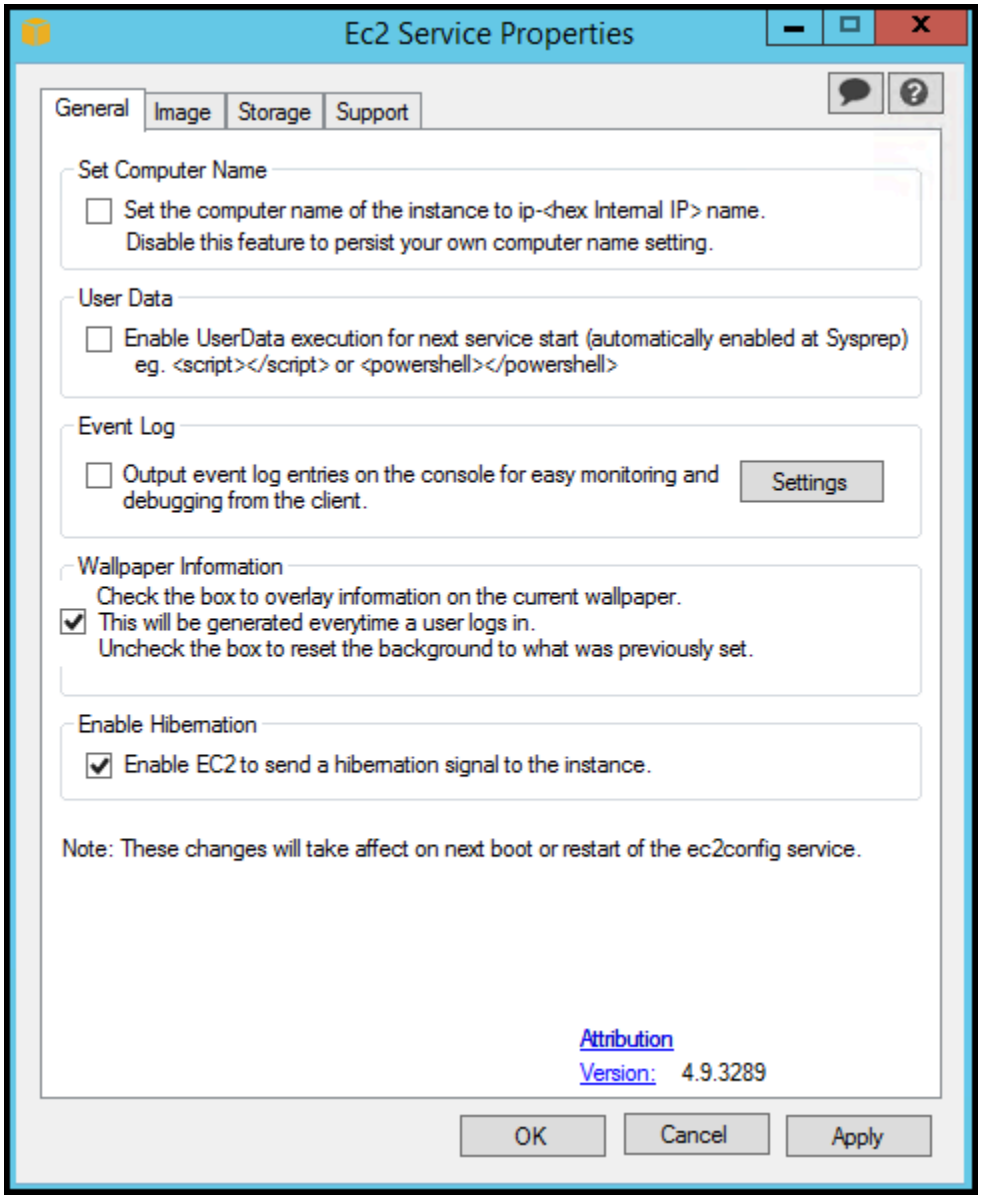
Si crea una AMI desde una instancia después de actualizar su configuración, la nueva configuración se aplica a cualquier instancia que se lance desde la nueva AMI. Para obtener información acerca de la creación de una AMI, consulte Creación de una AMI basada en Amazon EBS.

Propiedades de EC2

El siguiente procedimiento describe cómo utilizar el cuadro de diálogo Ec2 Service Properties (Propiedades del servicio de Ec2) para habilitar o deshabilitar opciones de configuración.

Para cambiar la configuración mediante el cuadro de diálogo Ec2 Service Properties (Propiedades del servicio de Ec2)

1. Lance y conéctese a la instancia de Windows.
2. En el menú Inicio haga clic en Todos los programas y, a continuación, en EC2ConfigService Settings (Configuración de Ec2ConfigService).



3. En la pestaña General del cuadro de diálogo EC2 Service Properties (Propiedades del servicio de EC2), puede habilitar o deshabilitar las siguientes opciones de configuración.

   Set Computer Name (Establecer nombre del equipo)

   Si se habilita esta opción (está deshabilitada de forma predeterminada), el nombre de host se compara con la dirección IP interna actual en cada arranque; si el nombre de host y la dirección IP interna no coinciden, se restablece el nombre de host para que contenga la dirección IP interna y, a continuación, el sistema se reinicia para obtener el nuevo nombre de host. Si desea establecer su propio nombre de host o evitar que se modifique su nombre de host existente, no habilite esta opción.

User Data (Datos de usuario)

La ejecución de datos de usuario le permite especificar scripts en los metadatos de la instancia. De forma predeterminada, estos scripts se ejecutan durante la inicialización inicial. También puede configurarlos para ejecutarse la próxima vez que se inicie o se reinicie la instancia, o bien cada vez que esto ocurra.

Si tiene un script grande, le recomendamos utilizar los datos de usuario para descargarlo y luego ejecutarlo.

Para obtener más información, consulte Ejecución de datos de usuario.

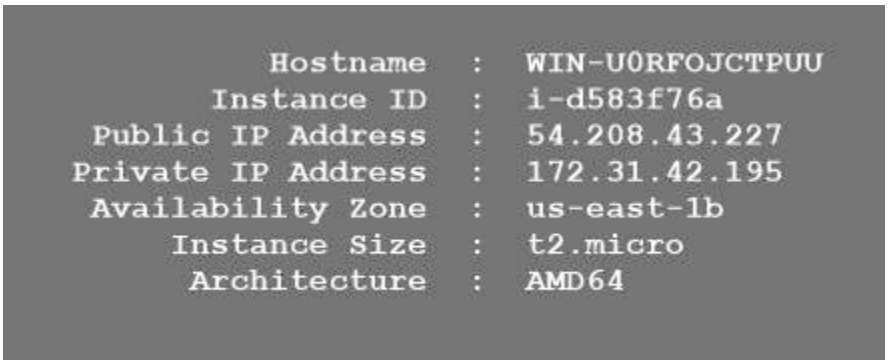
Event Log (Registro de eventos)

Utilice esta opción para mostrar las entradas de registro de eventos en la consola durante el arranque para una monitorización y depuración sencillas.

Haga clic en Settings (Configuración) para especificar filtros para las entradas de registro enviadas a la consola. El filtro predeterminado envía las tres entradas de error más recientes del registro de eventos del sistema a la consola.

Wallpaper Information (Información en el fondo de pantalla)

Utilice esta opción para mostrar la información del sistema en el fondo del escritorio. A continuación se muestra un ejemplo de la información mostrada en el fondo del escritorio.

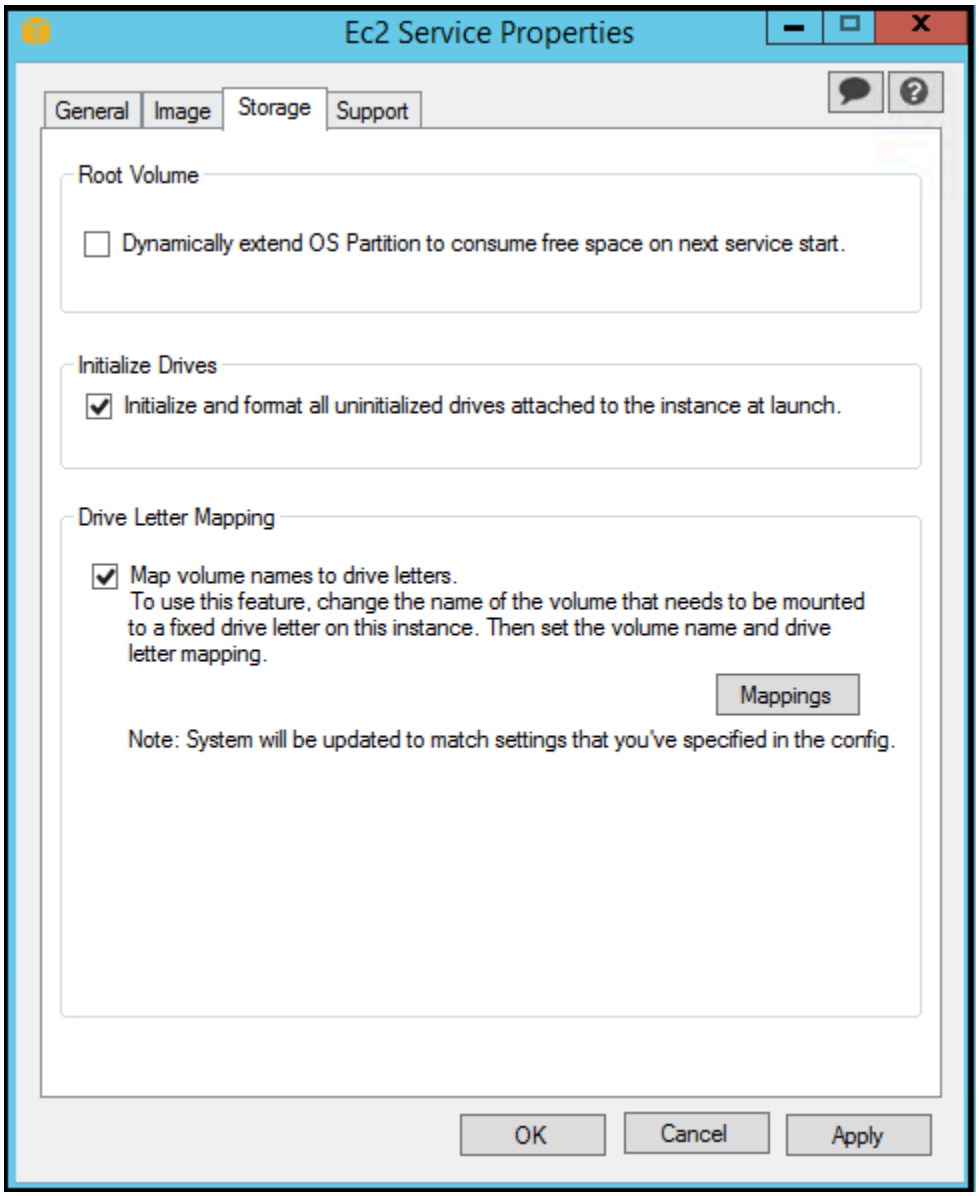


La información mostrada en el fondo del escritorio es controlada por el archivo de configuración `EC2ConfigService\Settings\WallpaperSettings.xml`.

Enable Hibernation (Habilitar la hibernación)

Utilice esta opción para permitir que EC2 indique al sistema operativo que realice la hibernación.

4. Haga clic en la pestaña Storage (Almacenamiento). Puede habilitar o deshabilitar las siguientes opciones de configuración.



Root Volume (Volumen raíz)

Esta opción amplía dinámicamente Disco 0/Volumen 0 para incluir cualquier espacio sin particionar. Esto puede resultar útil cuando la instancia se arranca desde un volumen de dispositivo raíz con un tamaño personalizado.

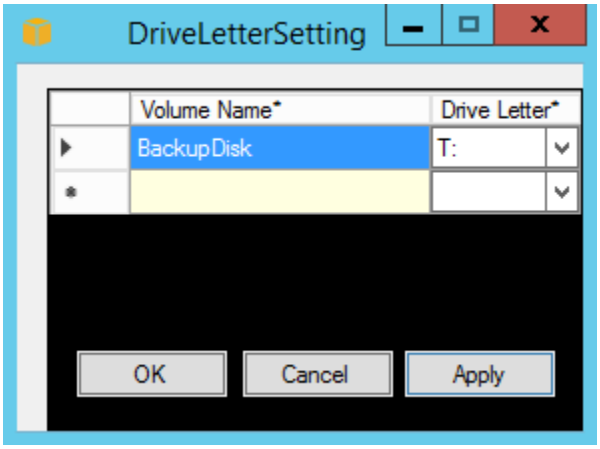
Initialize Drives (Inicializar unidades)

Esta opción formatea y monta todos los volúmenes adjuntos a la instancia durante el inicio.

Drive Letter Mapping (Mapeos de letras de unidad)

El sistema mapea los volúmenes adjuntos a una instancia en letras de unidad. Para volúmenes de Amazon EBS, la opción predeterminada es asignar letras de unidad de la D: a la Z:. Para volúmenes del almacén de instancias, la opción predeterminada depende del controlador. AWS Los controladores PV y Citrix PV asignan a los volúmenes de almacén de instancias letras de unidad de la Z: a la A:. Los controladores Red Hat asignan a los volúmenes de almacén de instancias letras de unidad de la D: a la Z:.

Para elegir las letras de unidad para sus volúmenes, haga clic en Mappings (Mapeos). En el cuadro de diálogo DriveLetterSetting, especifique los valores de Volume Name (Nombre del volumen) y Drive Letter (Letra de unidad) para cada volumen, haga clic en Apply (Aplicar) y, a continuación, haga clic en OK (Aceptar). Le recomendamos que seleccione letras de unidad de forma que no produzcan conflictos con otras letras que podrían estar en uso, por ejemplo, utilizando letras intermedias del alfabeto.



Cuando haya especificado un mapeo de letras de unidad y adjuntado un volumen con la misma etiqueta que uno de los nombres de volumen que especificó, EC2Config asigna automáticamente la letra de unidad especificada a dicho volumen. Sin embargo, si la letra de unidad ya está en uso, el mapeo de letras de unidad falla. Tenga en cuenta que EC2Config no cambia las letras de unidad de volúmenes que ya estuvieran montados cuando especificó el mapeo de letras de unidad.

5. Para guardar la configuración y seguir utilizándola a partir de ese momento, haga clic en OK (Aceptar) para cerrar el cuadro de diálogo EC2 Service Properties (Propiedades del servicio de EC2). Si ha terminado de personalizar la instancia y desea crear una AMI a partir de ella, consulte Creación de una AMI con Windows Sysprep.

Archivos de configuración de EC2Config

Los archivos de configuración controlan la operación del servicio EC2Config. Estos archivos están ubicados en el directorio `C:\Program Files\Amazon\Ec2ConfigService\Settings`:

- `ActivationSettings.xml`—controla la activación del producto mediante un servidor de administración de claves (AWS KMS).
- `AWS.EC2.Windows.CloudWatch.json` — controla qué contadores de rendimiento enviar a CloudWatch y qué registros enviar a CloudWatch Logs.
- `BundleConfig.xml` — controla cómo EC2Config prepara una instancia con respaldo en el almacén de instancias para la creación de AMI.
- `Config.xml` — controla la configuración principal.
- `DriveLetterConfig.xml` — controla los mapeos de letras de unidad.
- `EventLogConfig.xml` — controla la información del registro de eventos que se muestra en la consola durante el arranque de la instancia.
- `WallpaperSettings.xml` — controla la información que se muestra en el fondo del escritorio.

ActivationSettings.xml

Este archivo contiene la configuración que controla la activación del producto. Cuando Windows arranca, el servicio EC2Config comprueba si Windows ya está activado. Si Windows no está activado aún, intenta activarlo al buscar el servidor AWS KMS especificado.

- `SetAutodiscover`: indica si debe detectarse un AWS KMS automáticamente.
- `TargetKMSServer`—almacena la dirección IP privada de un AWS KMS. El AWS KMS debe estar en la misma región que la instancia.
- `DiscoverFromZone`: descubre el servidor AWS KMS a partir de la zona DNS especificada.
- `ReadFromUserData`: obtiene el servidor AWS KMS de UserData.
- `LegacySearchZones`: descubre el servidor AWS KMS a partir de la zona DNS especificada.
- `DoActivate` — intenta la activación utilizando la configuración especificada en la sección. Este valor puede ser `true` o `false`.
- `LogResultToConsole` — muestra el resultado en la consola.

BundleConfig.xml

Este archivo contiene la configuración que controla cómo EC2Config prepara una instancia para la creación de AMI.

- `AutoSysprep` — indica si se debe utilizar Sysprep automáticamente. Para utilizar Sysprep, cambie el valor a `Yes`.
- `SetRDPCertificate` — establece un certificado autofirmado en el servidor de Escritorio remoto. Esto le permite utilizar el RDP de forma segura para conectarse a las instancias. Si las nuevas instancias necesitan tener el certificado, cambie el valor a `Yes`.

  Esta configuración no se utiliza para instancias con versiones del sistema operativo anteriores a Windows Server 2016 porque dichos sistemas operativos pueden generar sus propios certificados.
- `SetPasswordAfterSysprep` — establece una contraseña aleatoria para una instancia recién iniciada, la cifra con la clave de inicialización del usuario y devuelve la contraseña cifrada a la consola. Si las nuevas instancias no deben configurarse con una contraseña cifrada aleatoria, cambie el valor de esta configuración a `No`.

Config.xml

Complementos

- `Ec2SetPassword` — genera una contraseña cifrada aleatoria cada vez que se inicia una instancia. Esta característica se deshabilita de forma predeterminada tras el primer inicialización para que la contraseña establecida por el usuario no cambie al reiniciarse la instancia. Para continuar generando contraseñas cada vez que lance una instancia, cambie esta opción a `Enabled`.

  Esta opción es importante si está pensando en crear una AMI a partir de la instancia.
- `Ec2SetComputerName` — establece el nombre de host de la instancia como un nombre único basado en la dirección IP de la instancia y la reinicia. Si desea establecer su propio nombre de host o evitar que se modifique su nombre de host existente, debe deshabilitar esta opción.
- `Ec2InitializeDrives` — inicializa y formatea todos los volúmenes durante el inicio. Esta característica está habilitada de forma predeterminada.
- `Ec2EventLog` — muestra las entradas del registro de eventos en la consola. De forma predeterminada, se muestran las tres entradas de error más recientes del registro de eventos del sistema. Para especificar las entradas del registro de eventos que desea que se muestren, edite

archivo `EventLogConfig.xml` ubicado en el directorio `EC2ConfigService\Settings`. Para obtener más información acerca de la configuración de este archivo, consulte Eventlog Key en la biblioteca de MSDN.

- `Ec2ConfigureRDP` — configura un certificado autofirmado en la instancia para que los usuarios puedan obtener acceso de forma segura a la instancia mediante el Escritorio remoto. Esta configuración no se utiliza para instancias con versiones del sistema operativo anteriores a Windows Server 2016 porque dichos sistemas operativos pueden generar sus propios certificados.
- `Ec2OutputRDPCert` — muestra la información del certificado de Escritorio remoto en la consola para que el usuario pueda cotejarla con la de la huella digital.
- `Ec2SetDriveLetter` — establece las letras de unidad de los volúmenes montados en función de la configuración definida por el usuario. De forma predeterminada, cuando un volumen de Amazon EBS se adjunta a una instancia, puede montarse en la letra de unidad de la instancia. Para especificar los mapeos de letras de unidad, edite archivo `DriveLetterConfig.xml` ubicado en el directorio `EC2ConfigService\Settings`.
- `Ec2WindowsActivate` — el complemento gestiona la activación de Windows. En primer lugar, comprueba si Windows está activado. Si no es así, actualiza la configuración de cliente de AWS KMS y, a continuación, activa Windows.

  Para modificar la configuración de AWS KMS, edite el archivo `ActivationSettings.xml` ubicado en el directorio `EC2ConfigService\Settings`.
- `Ec2DynamicBootVolumeSize` — amplía Disco 0/Volumen 0 para incluir cualquier espacio sin particionar.
- `Ec2HandleUserData` — Crean y ejecutan scripts creados por el usuario durante el primer inicialización de una instancia tras ejecutar Sysprep. Los comandos integrados en etiquetas de script se guardan en un archivo de procesamiento por lotes, mientras que los comandos integrados en etiquetas de PowerShell se guardan en un archivo .ps1 (lo que corresponde a la casilla de verificación User Data (Datos del usuario) del cuadro de diálogo Ec2 Service Properties (Propiedades del servicio EC2)).
- `Ec2ElasticGpuSetup` — instala el paquete de software de GPU elástica si la instancia está asociada a una GPU elástica.
- `Ec2FeatureLogging` — envía el estado de instalación de características de Windows y el estado del servicio correspondiente a la consola. Compatible únicamente con la características Hyper-V de Microsoft y el servicio vmms correspondiente.

Configuración global

- `ManageShutdown` — garantiza que las instancias iniciadas desde AMI con respaldo en el almacén de instancias no se terminen mientras Sysprep se está ejecutando.
- `SetDnsSuffixList` — establece el sufijo DNS del adaptador de red de Amazon EC2. Este permite la resolución de DNS de servidores que se ejecuten en Amazon EC2 sin proporcionar el nombre completo del dominio.

> **Note**
>
> Esto agrega una búsqueda de sufijos de DNS para el siguiente dominio y configura otros sufijos estándar. Para obtener más información acerca de cómo los agentes de inicialización configuran los sufijos de DNS, consulte Configuración del sufijo de DNS para los agentes de inicialización de Windows.
>
> ```
> region.ec2-utilities.amazonaws.com
> ```

- `WaitForMetaDataAvailable` — se asegura de que el servicio EC2Config esperará a que los metadatos estén accesibles y a que la red esté disponible antes de continuar con el arranque. Esta comprobación garantiza que EC2Config pueda obtener información de metadatos para la activación y otros complementos.
- `ShouldAddRoutes` — añade una ruta personalizada en el adaptador de red principal para habilitar las siguientes direcciones IP cuando se adjuntan varias NIC: 169.254.169.250, 169.254.169.251 y 169.254.169.254. Estas direcciones las utiliza la activación de Windows y cuando se obtiene acceso a los metadatos de la instancia.
- `RemoveCredentialsfromSyspreponStartup` — elimina la contraseña del administrador de `Sysprep.xml` la próxima vez que se inicia el servicio. Para asegurarse de que esta contraseña persiste, edite esta configuración.

DriveLetterConfig.xml

Este archivo contiene la configuración que controla los mapeos de letras de unidad. De forma predeterminada, un volumen se puede asignar en cualquier letra de unidad disponible. Puede montar un volumen en una letra de unidad en particular del modo siguiente.

```
<?xml version="1.0" standalone="yes"?>
<DriveLetterMapping>
  <Mapping>
    <VolumeName></VolumeName>
```

```
    <DriveLetter></DriveLetter>
  </Mapping>
  . . .
  <Mapping>
    <VolumeName></VolumeName>
    <DriveLetter></DriveLetter>
  </Mapping>
</DriveLetterMapping>
```

- `VolumeName` — la etiqueta del volumen. Por ejemplo, *`My Volume`*. Para especificar un mapeo para un volumen de almacén de instancias, utilice la etiqueta `Temporary Storage X`, donde `X` es un número del 0 al 25.
- `DriveLetter` — la letra de unidad. Por ejemplo, *`M:`*. Si la letra de unidad ya está en uso, el mapeo falla.

EventLogConfig.xml

Este archivo contiene la configuración que controla la información del registro de eventos que se muestra en la consola durante el arranque de la instancia. De forma predeterminada, se muestran las tres entradas de error más recientes del registro de eventos del sistema.

- `Category` — la clave del registro de eventos que se va a monitorizar.
- `ErrorType`—el tipo de evento (por ejemplo, , o, `Error`, `Warning`, `Information`.)
- `NumEntries` — el número de eventos almacenado para esta categoría.
- `LastMessageTime` — para evitar que se envíe el mismo mensaje repetidamente, el servicio actualiza este valor cada vez que envía un mensaje.
- `AppName` — el origen de eventos o la aplicación que registró el evento.

WallpaperSettings.xml

Este archivo contiene la configuración que controla la información que se muestra en fondo del escritorio. De forma predeterminada, se muestra la siguiente información.

- `Hostname` — muestra el nombre del equipo.
- `Instance ID` — muestra el ID de la instancia.
- `Public IP Address` — muestra la dirección IP pública de la instancia.
- `Private IP Address` — muestra la dirección IP privada de la instancia.

- `Availability Zone` — muestra la zona de disponibilidad en la que se ejecuta la instancia.
- `Instance Size` — muestra el tipo de instancia.
- `Architecture` — muestra la configuración de la variable de entorno `PROCESSOR_ARCHITECTURE`.

Puede eliminar cualquier información que se muestre de forma predetermina eliminando esta entrada. Puede añadir metadatos de instancia adicionales para que se muestren del modo siguiente.

```
<WallpaperInformation>
  <name>display_name</name>
  <source>metadata</source>
  <identifier>meta-data/path</identifier>
</WallpaperInformation>
```

Puede añadir variables de entorno del sistema adicionales para que se muestren del modo siguiente.

```
<WallpaperInformation>
  <name>display_name</name>
  <source>EnvironmentVariable</source>
  <identifier>variable-name</identifier>
</WallpaperInformation>
```

InitializeDrivesSettings.xml

Este archivo contiene la configuración que controla cómo EC2Config inicializa las unidades.

De forma predeterminada, EC2Config inicializa las unidades que no se pusieron online mediante el sistema operativo. Puede personalizar el complemento del modo siguiente.

```
<InitializeDrivesSettings>
    <SettingsGroup>setting</SettingsGroup>
</InitializeDrivesSettings>
```

Utilice un grupo de configuración para especificar cómo desea inicializar las unidades:

FormatWithTRIM

Habilita el comando TRIM al formatear unidades. Después de formatear e inicializar una unidad, el sistema restablece la configuración TRIM.

A partir de la versión 3.18 de EC2Config, el comando TRIM se deshabilita de forma predeterminada durante la operación de formateo de discos. Esto mejora los tiempos de formateo. Utilice esta opción para habilitar TRIM durante la operación de formateo de discos para la versión 3.18 y posteriores de EC2Config.

FormatWithoutTRIM

Deshabilita el comando TRIM durante el formateo de unidades disco y mejora los tiempos de formateo en Windows. Después de formatear e inicializar una unidad, el sistema restablece la configuración TRIM.

DisableInitializeDrives

Deshabilita el formateo para nuevas unidades. Utilice esta opción para inicializar unidades manualmente.

Configurar los ajustes proxy del servicio EC2Config

Puede configurar el servicio EC2Config para que se comunique a través de un proxy mediante uno de los siguientes métodos: el SDK de AWS para .NET, el elemento `system.net` o Microsoft Group Policy e Internet Explorer. El método recomendado es el SDK de AWS para .NET porque puede especificar credenciales de inicio de sesión.

Métodos

- Configurar los ajustes proxy utilizando AWS SDK for .NET (preferido)
- Configurar los ajustes proxy utilizando el elemento system.net
- Configurar los ajustes proxy utilizando Microsoft Group Policy y Microsoft Internet Explorer

Configurar los ajustes proxy utilizando AWS SDK for .NET (preferido)

Puede configurar la configuración del proxy para el servicio EC2Config especificando el elemento `proxy` en el archivo `Ec2Config.exe.config`. Para obtener más información, consulte Referencia de los archivos de configuración para el SDK de AWS para .NET.

Para especificar el elemento del proxy en Ec2Config.exe.config

1. Edite el archivo `Ec2Config.exe.config` de una instancia en la que desee que el servicio EC2Config se comunique a través de un proxy. De forma predeterminada, el archivo se ubica en el siguiente directorio: `%ProgramFiles%\Amazon\Ec2ConfigService`.

2. Añada el siguiente elemento `aws` a `configSections`. No lo agregue a `sectionGroups` existentes.

   Para la versión 3.17 o anterior de EC2Config

   ```
   <configSections>
      <section name="aws" type="Amazon.AWSSection, AWSSDK"/>
   </configSections>
   ```

   Para la versión 3.18 o posterior de EC2Config

   ```
   <configSections>
        <section name="aws" type="Amazon.AWSSection, AWSSDK.Core"/>
   </configSections>
   ```

3. Añada el siguiente elemento `aws` al archivo `Ec2Config.exe.config`.

   ```
   <aws>
      <proxy
        host="string value"
        port="string value"
        username="string value"
        password="string value" />
   </aws>
   ```

4. Guarde los cambios.

Configurar los ajustes proxy utilizando el elemento system.net

Puede especificar la configuración del proxy en un elemento `system.net` del archivo `Ec2Config.exe.config`. Para obtener más información, consulte defaultProxy Element (Network Settings) en MSDN.

Para especificar el elemento system.net en Ec2Config.exe.config

1. Edite el archivo `Ec2Config.exe.config` de una instancia en la que desee que el servicio EC2Config se comunique a través de un proxy. De forma predeterminada, el archivo se ubica en el siguiente directorio: `%ProgramFiles%\Amazon\Ec2ConfigService`.
2. Añada una entrada `defaultProxy` a `system.net`. Para obtener más información, consulte defaultProxy Element (Network Settings) en MSDN.

Por ejemplo, la siguiente configuración dirige todo el tráfico para utilizar el proxy que está actualmente configurado para Internet Explorer, a excepción de los metadatos y el tráfico de licencia, que omitirá el proxy.

```
<defaultProxy>
    <proxy usesystemdefault="true" />
    <bypasslist>
        <add address="169.254.169.250" />
        <add address="169.254.169.251" />
        <add address="169.254.169.254" />
        <add address="[fd00:ec2::250]" />
        <add address="[fd00:ec2::254]" />
    </bypasslist>
</defaultProxy>
```

3. Guarde los cambios.

Configurar los ajustes proxy utilizando Microsoft Group Policy y Microsoft Internet Explorer

El servicio EC2Config se ejecuta en la cuenta de usuario del sistema local. Puede especificar configuración del proxy para toda la instancia para esta cuenta en Internet Explorer una vez que haya cambiado la configuración de políticas de grupo en la instancia.

Para configurar los ajustes del proxy mediante Group Policy e Internet Explorer

1. En una instancia en la que desee que el servicio EC2Config se comunique a través de un proxy, abra un símbolo del sistema como administrador, escriba **`gpedit.msc`** y pulse Intro.
2. En el editor de directivas de grupo local, en Directiva Equipo local, elija Configuración del equipo, Plantillas administrativas, Componentes de Windows, Internet Explorer.
3. En el panel de la derecha, elija Configuración de proxy por equipo y no por usuario y, a continuación, elija Editar configuración de directiva.
4. Elija Habilitada y, a continuación, elija Aplicar.
5. Abra Internet Explorer y, a continuación, elija el botón Herramientas.
6. Elija Opciones de Internet y, a continuación, elija la pestaña Conexiones.
7. Elija Configuración de LAN.
8. En Servidor proxy, elija la opción Usar un servidor proxy para la LAN.
9. Especifique la dirección y la información del puerto y, a continuación, elija Aceptar.

Historial de versión de EC2Config

Las AMI de Windows anterior a Windows Server 2016 incluyen un servicio opcional llamado servicio EC2Config (`EC2Config.exe`). EC2Config se inicia cuando la instancia arranca y realiza tareas durante el inicio, así como cada vez que detiene o inicia la instancia.

Puede recibir notificaciones cuando se publiquen nuevas versiones del servicio EC2Config. Para obtener más información, consulte Suscribirse a las notificaciones del servicio EC2Config.

En la siguiente tabla se describen las versiones de EC2Config publicadas. Para obtener más información acerca de las actualizaciones del SSM Agent, consulte Notas de la versión del SSM Agent de Administrador de sistemas.

Versión	Detalles	Fecha de la versión
4.9.5554	• Limite la devolución de nombres de dominio en función de la entrada de registro: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters\DomainNameDevolutionLevel` . • Nueva versión de SSM Agent `3.2.1630.0` .	4 de octubre de 2023
4.9.5467	• Se agregó la capacidad de reintento para detectar el puerto de la consola. • Nueva versión de SSM Agent `3.1.2282.0` .	1 de agosto de 2023
4.9.5288	• Se actualizó el SDK principal de AWS a la versión `3.7.103.23` . • Se solucionó el problema por el que el documento de SSM `AWS-UpdateEC2Config` no se actualizaba a `EC2Config` en las instancias habilitadas solo con IMDSv2. • Nueva versión de SSM Agent `3.1.2144.0` .	8 de marzo de 2023

Versión	Detalles	Fecha de la versión
4.9.5231	• Nueva versión de SSM Agent 3.1.1927.0.	14 de febrero de 2023
4.9.5103	• Se solucionó un problema por el que los volúmenes efímeros se identificaban incorrectamente en las familias de instancias r5d e i4i. • Nueva versión de SSM Agent 3.1.1856.0.	5 de diciembre de 2022
4.9.5064	• Se actualizó para usar la información del segmento PCI con el fin de seleccionar el puerto de la consola. • Se han firmado scripts de PowerShell y se han agregado encabezados de derechos de autor. • Se corrigió la lógica de selección del adaptador de red principal. • Nueva versión de SSM Agent 3.1.1732.0.	16 de noviembre de 2022
4.9.4588	• Se actualizó la lógica de espera de IMDS para realizar solo solicitudes IMDSv2. • Se agregó la biblioteca compartida libec2launch.dll launch-agent. • Nueva versión de SSM Agent 3.1.1188.0.	31 de mayo de 2022

Versión	Detalles	Fecha de la versión
4.9.4556	• Se agregó lógica de espera para garantizar la inicialización completa de la NIC antes de su uso. • La nueva versión de Log4Net 2.0.14.0 recibe la revisión de seguridad. • La nueva versión de SSM Agent 3.1.1045.0 recibe la revisión de seguridad.	1 de marzo de 2022
4.9.4536	• Se corrigió el problema por el cual los datos de usuario se bloquean cuando falta la carpeta Temp. • Nueva versión de SSM Agent 3.1.804.0.	31 de enero de 2022
4.9.4508	• Se ha corregido el problema para calcular correctamente la ruta de script de diskpart. • Nueva versión de SSM Agent 3.1.338.0.	6 de octubre de 2021
4.9.4500	• `Install-EgpuManagerConfig` actualizada con soporte de IMDS v2. • Enlaces web actualizados para utilizar https. • Nueva versión de SSM Agent 3.1.282.0	7 de septiembre de 2021
4.9.4419	• Se ha corregido la lógica alternativa 1 de la versión IMDS • Se actualizó todo el uso del directorio temporal de Windows al directorio temporal de EC2Config • Nueva versión de SSM Agent 3.0.1124.0	2 de junio de 2021

Versión	Detalles	Fecha de la versión
4.9.4381	• Se agregó soporte para el esquema de documento SSM, versión 2.2, en EC2Configupdater • Se ha añadido la versión del paquete de Nitro Enclaves AWS al registro de la consola • Nueva versión de SSM Agent 3.0.529.0	4 de mayo de 2021
4.9.4326	• Se han eliminado todos los vínculos en la interfaz de usuario de configuración • Esta es la última versión de EC2Config que admite Windows Server 2008.	3 de marzo de 2021
4.9.4279	• Se corrigió el problema de seguridad relacionado `Ec2Config Monitor` con la tarea programada • Se corrigió un problema de asignación de letras de unidad y de recuento de discos efímeros incorrecto • Se agregó `OsCurrentBuild` y `OsReleaseId` a la salida de consola • Nueva versión de SSM Agent 2.3.871.0	11 de diciembre de 2020
4.9.4222	• Se ha corregido la lógica alternativa 1 de la versión IMDS • Nueva versión de SSM Agent (2.3.842.0)	7 de abril de 2020
4.9.4122	• Se ha agregado compatibilidad con IMDS v2 • Nueva versión de SSM Agent (2.3.814.0)	4 de marzo de 2020
4.9.3865	• Se ha solucionado el problema de detección del puerto COM para Windows Server 2008 R2 en instancias metal • Nueva versión de SSM Agent (2.3.722.0)	31 de octubre de 2019
4.9.3519	• Nueva versión de SSM Agent (2.3.634.0)	18 de junio de 2019

Versión	Detalles	Fecha de la versión
4.9.3429	• Nueva versión de SSM Agent (2.3.542.0)	25 de abril de 2019
4.9.3289	• Nueva versión de SSM Agent 2.3.444.0	11 de febrero de 2019
4.9.3270	• Se ha añadido un complemento para establecer que el monitor debe apagarse nunca para corregir problemas de ACPI. • La versión y la edición de SQL Server se escriben en la consola. • Nueva versión de SSM Agent 2.3.415.0	22 de enero de 2019
4.9.3230	• Se ha actualizado la descripción del mapeo de letras de unidad para ceñirse mejor a la funcionalidad • Nueva versión de SSM Agent 2.3.372.0	10 de enero de 2019
4.9.3160	• Incremento del tiempo de espera del NIC primario. • Configuración predeterminada añadida para la configuración de RSS y Recibir colas para dispositivos ENA. • Hibernación deshabilitada durante Sysprep. • Nueva versión de SSM Agent 2.3.344.0 • El SDK de AWS actualizado a 3.3.29.13	15 de diciembre de 2018
4.9.3067	• Mejoras en la hibernación de instancias • Nueva versión de SSM Agent 2.3.235.0	8 de noviembre de 2018
4.9.3034	• Ruta 169.254.169.253/32 añadida para el servidor DNS • Nueva versión de SSM Agent 2.3.193.0	24 de octubre de 2018

Versión	Detalles	Fecha de la versión
4.9.2986	• Firma añadida para todos los binarios relacionados con EC2Config • Nueva versión de SSM Agent 2.3.136.0	11 de octubre de 2018
4.9.2953	Nueva versión de SSM Agent (2.3.117.0)	2 de octubre de 2018
4.9.2926	Nueva versión de SSM Agent (2.3.68.0)	18 de septiembre de 2018
4.9.2905	• Nueva versión de SSM Agent (2.3.50.0) • Se ha añadido la ruta 169.254.169.123/32 al servicio de hora AMZN • Se ha añadido la ruta 169.254.169.249/32 al servicio de licencias GRID. • Se ha corregido un problema que hacía que los volúmenes NVMe de EBS se marcaran como efímeros.	17 de septiembre de 2018
4.9.2854	Nueva versión de SSM Agent (2.3.13.0)	17 de agosto de 2018
4.9.2831	Nueva versión de SSM Agent (2.2.916.0)	7 de agosto de 2018
4.9.2818	Nueva versión de SSM Agent (2.2.902.0)	31 de julio de 2018
4.9.2756	Nueva versión de SSM Agent (2.2.800.0)	27 de junio de 2018
4.9.2688	Nueva versión de SSM Agent (2.2.607.0)	25 de mayo de 2018

Versión	Detalles	Fecha de la versión
4.9.2660	Nueva versión de SSM Agent (2.2.546.0)	11 de mayo de 2018
4.9.2644	Nueva versión de SSM Agent (2.2.493.0)	26 de abril de 2018
4.9.2586	Nueva versión de SSM Agent (2.2.392.0)	28 de marzo de 2018
4.9.2565	• Nueva versión de SSM Agent (2.2.355.0) • Se ha corregido un error en las instancias M5 y C5 (no se pueden encontrar los controladores PV) • Se ha añadido el registro en la consola para los tipos de instancias, los controladores PV más recientes y los controladores NVMe	13 de marzo de 2018
4.9.2549	Nueva versión de SSM Agent (2.2.325.0)	8 de marzo de 2018
4.9.2461	Nueva versión de SSM Agent (2.2.257.0)	15 de febrero de 2018
4.9.2439	Nueva versión de SSM Agent (2.2.191.0)	6 de febrero de 2018
4.9.2400	Nueva versión de SSM Agent (2.2.160.0)	16 de enero de 2018
4.9.2327	• Nueva versión de SSM Agent (2.2.120.0) • Se ha añadido la detección del puerto COM en las instancias bare metal de Amazon EC2 • Se ha añadido el registro de estado de Hyper-V en la instancias bare metal de Amazon EC2	2 de enero de 2018

Versión	Detalles	Fecha de la versión
4.9.2294	Nueva versión de SSM Agent (2.2.103.0)	4 de diciembre de 2017
4.9.2262	Nueva versión de SSM Agent (2.2.93.0)	15 de noviembre de 2017
4.9.2246	Nueva versión de SSM Agent (2.2.82.0)	11 de noviembre de 2017
4.9.2218	Nueva versión de SSM Agent (2.2.64.0)	29 de octubre de 2017
4.9.2212	Nueva versión de SSM Agent (2.2.58.0)	23 de octubre de 2017
4.9.2203	Nueva versión de SSM Agent (2.2.45.0)	19 de octubre de 2017
4.9.2188	Nueva versión de SSM Agent (2.2.30.0)	10 de octubre de 2017
4.9.2180	• Nueva versión de SSM Agent (2.2.24.0) • Se ha añadido el complemento de GPU elástica para las instancias de GPU.	5 de octubre de 2017
4.9.2143	Nueva versión de SSM Agent (2.2.16.0)	1 de octubre de 2017
4.9.2140	Nueva versión de SSM Agent (2.1.10.0)	
4.9.2130	Nueva versión de SSM Agent (2.1.4.0)	

Versión	Detalles	Fecha de la versión
4.9.2106	Nueva versión de SSM Agent (2.0.952.0)	
4.9.2061	Nueva versión de SSM Agent (2.0.922.0)	
4.9.2047	Nueva versión de SSM Agent (2.0.913.0)	
4.9.2031	Nueva versión de SSM Agent (2.0.902.0)	
4.9.2016	• Nueva versión de SSM Agent (2.0.879.0) • Se ha corregido la ruta del directorio de CloudWatch Logs en Windows Server 2003.	
4.9.1981	• Nueva versión de SSM Agent (2.0.847.0) • Se ha corregido el problema de la generación de `important.txt` en volúmenes de EBS.	
4.9.1964	Nueva versión de SSM Agent (2.0.842.0)	
4.9.1951	• Nueva versión de SSM Agent (2.0.834.0) • Se ha corregido el problema del no asignación de letras de unidad desde la Z: para unidades efímeras.	
4.9.1925	• Nueva versión de SSM Agent (2.0.822.0) • [Error] Esta versión no es una actualización válida de SSM Agent v4.9.1775.	
4.9.1900	Nueva versión de SSM Agent (2.0.805.0)	

Versión	Detalles	Fecha de la versión
4.9.1876	• Nueva versión de SSM Agent (2.0.796.0) • Se ha corregido el problema del redireccionamiento de salida/error para la ejecución de datos de usuario de administrador.	
4.9.1863	• Nueva versión de SSM Agent (2.0.790.0) • Se han corregido los problemas de la conexión de varios volúmenes de EBS a una instancia Amazon EC2. • Se ha mejorado CloudWatch para seguir una ruta de configuración, manteniendo la compatibilidad con versiones anteriores.	
4.9.1791	Nueva versión de SSM Agent (2.0.767.0)	
4.9.1775	Nueva versión de SSM Agent (2.0.761.0)	
4.9.1752	Nueva versión de SSM Agent (2.0.755.0)	
4.9.1711	Nueva versión de SSM Agent (2.0.730.0)	
4.8.1676	Nueva versión de SSM Agent (2.0.716.0)	
4.7.1631	Nueva versión de SSM Agent (2.0.682.0)	
4.6.1579	• Nueva versión de SSM Agent (2.0.672.0) • Se ha corregido el problema de la actualización del agent en v4.3, v4.4 y v4.5	
4.5.1534	Nueva versión de SSM Agent (2.0.645.1)	
4.4.1503	Nueva versión de SSM Agent (2.0.633.0)	

Versión	Detalles	Fecha de la versión
4.3.1472	Nueva versión de SSM Agent (2.0.617.1)	
4.2.1442	Nueva versión de SSM Agent (2.0.599.0)	
4.1.1378	Nueva versión de SSM Agent (2.0.558.0)	
4.0.1343	• Run Command, State Manager, el agente de CloudWatch y la compatibilidad de unirse al dominio se han movido a otro agente llamado SSM Agent. El SSM Agent se instalará como parte de la actualización de EC2Config. Para obtener más información, consulte EC2Config y AWS Systems Manager. • Si tiene un proxy configurado en EC2Config, necesitará actualizar la configuración del proxy para SSM Agent antes de realizar la actualización. Si no actualiza la configuración del proxy, no podrá utilizar Ejecutar comando para administrar las instancias. Para evitarlo, consulte la siguiente información antes de actualizar a la nueva versión: Instalar y configurar el SSM Agent en instancias de Windows en la Guía del usuario de AWS Systems Manager. • Si habilitó la integración de CloudWatch en sus instancias anteriormente mediante un archivo de configuración local (`AWS.EC2.Windows.CloudWatch.json`), tendrá que configurar el archivo para que funcione con SSM Agent.	

Versión	Detalles	Fecha de la versión
3.19.1153	• Se ha vuelto a habilitar el complemento de activación para instancias con una configuración de AWS KMS anterior. Omita la activación para los usuarios de BYOL. • Se ha cambiado el comportamiento predeterminado de TRIM para que se deshabilite durante la operación de formateo de discos y se ha añadido FormatWithTRIM para anular el complemento InitializeDisks con datos de usuario.	
3.18.1118	• Se ha introducido una corrección para añadir rutas al adaptador de red principal de forma fiable. • Actualizaciones para mejorar la compatibilidad para los servicios de AWS.	
3.17.1032	• Se ha corregido el problema de la aparición de registros del sistema duplicados al establecer los filtros en la misma categoría. • Se han introducido correcciones para evitar bloqueos durante la inicialización de los discos.	
3.16.930	Se ha añadido compatibilidad para registrar el evento "Window is Ready to use" en el registro de eventos de Windows durante el inicio.	
3.15.880	Se ha introducido una corrección para permitir la carga de la salida de la ejecución de comandos de Systems Manager a nombres de buckets de S3 con el carácter ".".	

Versión	Detalles	Fecha de la versión
3.14.786	Se ha añadido compatibilidad para anular la configuración del complemento InitializeDisks. Por ejemplo: Para acelerar la inicialización de discos SSD, puede deshabilitar TRIM temporalmente especificándolo en los datos de usuario: <InitializeDrivesSettings><SettingsGroup>FormatWithoutTRIM</SettingsGroup></InitializeDrivesSettings	
3.13.727	Run Command de Systems Manager: se han introducido correcciones para procesar comandos de forma fiable tras reiniciarse Windows.	
3.12.649	• Se ha introducido una corrección para gestionar correctamente el reinicio cuando se ejecutan comandos/scripts. • Se ha introducido una corrección para cancelar comandos en ejecución de forma fiable. • Se ha añadido compatibilidad para cargar (opcionalmente) registros de MSI a S3 al instalar aplicaciones mediante Run Command de Systems Manager.	
3.11.521	• Se han introducido correcciones para permitir la generación de huellas digitales de RDP en Windows Server 2003. • Se han introducido correcciones para incluir la zona horaria y el desfase respecto a UTC en las líneas del registro de EC2Config. • Compatibilidad de Systems Manager para ejecutar comandos en paralelo. • Reversión del cambio anterior para poner los discos particionados online.	

Versión	Detalles	Fecha de la versión
3.10.442	• Se han corregido los errores de configuración de Systems Manager al instalar aplicaciones de MSI. • Se ha introducido una corrección para poner discos de almacenamiento online de forma fiable • Actualizaciones para mejorar la compatibilidad para los servicios de AWS.	
3.9.359	• Se ha introducido una corrección en el script post Sysprep para dejar la configuración de Windows Update en un estado predeterminado. • Se ha corregido el complemento de generación de contraseñ as para mejorar la fiabilidad a la hora de obtener la configura ción de la política de contraseñas GPO. • Se han restringido los permisos de las carpetas del registro de EC2Config/SSM para el grupo de administradores locales. • Actualizaciones para mejorar la compatibilidad para los servicios de AWS.	

Versión	Detalles	Fecha de la versión
3.8.294	• Se ha corregido un problema en CloudWatch que impedía la carga de registros cuando no estaban en la unidad principal. • Se ha mejorado el proceso de inicialización de discos añadiendo lógica de reintento. • Se ha añadido una mejor capacidad de gestión de errores cuando el complemento SetPassword fallaba ocasionalmente durante la creación de la AMI. • Actualizaciones para mejorar la compatibilidad para los servicios de AWS.	
3.7.308	• Se han introducido mejoras a la utilidad ec2config-cli para pruebas y solución de problemas de configuración dentro de la instancia. • Se ha impedido agregar rutas estáticas para AWS KMS y el servicio de metadatos en un adaptador OpenVPN. • Se ha corregido un problema por el que la ejecución de datos de usuario no respetaba la etiqueta ""persist". • Se ha mejorado la gestión de errores cuando el registro en la consola de EC2 no está disponible. • Actualizaciones para mejorar la compatibilidad para los servicios de AWS.	

Versión	Detalles	Fecha de la versión
3.6.269	• Se ha corregido la fiabilidad de la activación de Windows para que primero se utilice la dirección de enlace local 169.254.0 .250/251 para activar Windows mediante AWS KMS • Se ha mejorado la gestión de proxy para los casos de Systems Manager, activación de Windows e incorporación al dominio • Se ha corregido un problema por el que se añadían línea duplicadas de cuentas de usuario al archivo de respuestas de Sysprep	
3.5.228	• Se ha dado respuesta a un caso en el que el complemen to CloudWatch puede consumir una capacidad de CPU y memoria excesiva al leer registros de eventos de Windows • Se ha añadido un enlace a la documentación de configuración de CloudWatch en la interfaz de usuario de la configuración de EC2Config	
3.4.212	• Se han introducido correcciones en EC2Config al utilizarse en combinación con VM Import. • Se ha corregido un problema de nomenclatura de servicios en el instalador WiX.	

Versión	Detalles	Fecha de la versión
3.3.174	• Se ha mejorado la gestión de excepciones para Systems Manager y los errores de incorporación al dominio. • Se ha introducido un cambio para admitir el control de versiones de esquemas de SSM de Systems Manager. • Se ha corregido el formateo de discos efímeros en Win2K3. • Se ha introducido un cambio para admitir la configuración de tamaños de disco superiores a 2 TB. • Se ha reducido el uso de memoria virtual estableciendo la configuración predeterminada del modo GC. • Compatibilidad para descargar elementos de una ruta UNC con los complementos `aws:psModule` y `aws:application` . • Se ha mejorado el registro para el complemento de activación de Windows.	

Versión	Detalles	Fecha de la versión
3.2.97	• Mejoras de rendimiento mediante la carga retardada de conjuntos SSM de Systems Manager. • Se ha mejorado la gestión de excepciones para sysprep2008.xml con formato incorrecto. • Compatibilidad con líneas de comando para la configuración de “Apply” de Systems Manager. • Se ha introducido un cambio para admitir la incorporación al dominio cuando hay un cambio de nombre de equipo pendiente. • Compatibilidad para parámetros opcionales en el complemento `aws:applications` . • Compatibilidad para matrices de comandos en el complemento `aws:psModule` .	
3.0.54	• Habilitación de la compatibilidad con Systems Manager. • Incorporación al dominio automáticamente de las instancias de EC2 de Windows a un directorio de AWS mediante Systems Manager. • Configuración y carga de registros/métricas de CloudWatch mediante Systems Manager. • Instalación de módulos PowerShell mediante Systems Manager. • Instalación de aplicaciones de MSI mediante Systems Manager.	

Versión	Detalles	Fecha de la versión
2.4.233	• Se ha añadido una tarea programada para recuperar EC2Config tras un error de inicio del servicio. • Mejoras en los mensajes de error del registro de la consola. • Actualizaciones para mejorar la compatibilidad para los servicios de AWS.	
2.3.313	• Se ha corregido el problema del gran consumo de memoria en algunos casos cuando se habilita la opción de CloudWatch Logs. • Se ha corregido un error de actualización, de forma que las versiones de ec2config anteriores a 2.1.19 ya pueden actualizarse a la última versión. • Se ha actualizado la excepción de la apertura del puerto COM para que sea más sencilla y útil en los registros. • Se han deshabilitado los cambios de tamaño de la interfaz de usuario de Ec2configServiceSettings y se ha corregido la ubicación de la atribución y la versión en la interfaz de usuario.	
2.2.12	• Se gestiona NullPointerException mientras se consulta una clave de registro para determinar el estado de Windows Sysprep que devolvía null ocasionalmente. • Se han liberado recursos no administrados en el bloque finally.	
2.2.11	Se ha corregido un problema en el complemento de CloudWatch para administrar líneas de registro vacías.	

Versión	Detalles	Fecha de la versión
2.2.10	• Se ha eliminado la configuración de los valores de CloudWatch Logs mediante la interfaz de usuario. • Permitir a los usuarios definir la configuración de CloudWatch Logs en el archivo `%ProgramFiles%\Amazon\Ec2ConfigService\Settings\AWS.EC2.Windows.CloudWatch.json` para permitir futuras mejoras.	
2.2.9	Se ha corregido una excepción no administrada y se ha añadido registro.	
2.2.8	• Se ha corregido la comprobación de versiones de SO de Windows en el instalador de EC2Config para admitir Windows Server 2003 SP1 y posterior. • Se ha corregido la gestión del valor null al leer claves de registro relacionadas con la actualización de archivos de configuración de Sysprep.	
2.2.7	• Se ha agregado compatibilidad para que EC2Config se ejecute durante la ejecución de Sysprep en Windows 2008 y superior. • Se ha mejorado la gestión y el registro de excepciones para un mejor diagnóstico.	
2.2.6	• Se ha reducido la carga sobre la instancia y sobre CloudWatch Logs al cargar eventos del registro. • Se ha dado respuesta a un problema de actualización en el que el complemento de CloudWatch Logs no siempre permanecía habilitado	

Versión	Detalles	Fecha de la versión
2.2.5	• Se ha agregado compatibilidad para cargar registros al servicio de registro de CloudWatch. • Se ha corregido un problema de condición de carrera en el complemento Ec2OutputRDPCert • Se ha cambiado la opción de recuperación del servicio EC2Config para que se reinicie desde TakeNoAction • Se ha añadido más información sobre excepciones cuando EC2Config se bloquea	
2.2.4	• Se ha corregido una errata en PostSysprep.cmd • Se ha corregido el error por el que EC2Config no se adjunta al menú de inicio de OS2012+	

Versión	Detalles	Fecha de la versión
2.2.3	• Se ha añadido la opción de instalar EC2Config sin que el servicio comience inmediatamente tras la instalación. Para activarla, ejecute 'Ec2Install.exe start=false' en el símbolo del sistema • Se ha añadido un parámetro en el complemento del fondo de pantalla para controlar la opción de añadir/eliminar fondo de pantalla. Para activarlo, ejecute 'Ec2WallpaperInfo.exe set' o 'Ec2WallpaperInfo.exe revert' en el símbolo del sistema • Se ha añadido la comprobación de la clave RealTimeI sUniversal y la muestra de la configuración incorrecta de la clave de registro RealTimeIsUniveral en la consola • Se ha eliminado la dependencia de EC2Config en la carpeta temporal de Windows • Se ha eliminado la dependencia de la ejecución de UserData en .Net 3.5	
2.2.2	• Se ha añadido la comprobación del comportamiento de la detención de servicio para comprobar que los recursos se están publicando • Se ha corregido el problema de los prolongados tiempos de ejecución al incorporarse al dominio	

Versión	Detalles	Fecha de la versión
2.2.1	• Se ha actualizado el instalador para permitir actualizaciones de las versiones anteriores • Se ha corregido un error de Ec2WallpaperInfo en el entorno de .Net4.5 únicamente • Se ha corregido el error de la detección intermitente de controladores • Se ha añadido la opción de instalación en modo silencios o. Ejecute Ec2Install.exe con la opción '-q'. Por ejemplo, 'Ec2Install.exe -q'.	
2.2.0	• Se ha agregado compatibilidad con los entornos .Net4 y .Net4.5 únicamente • Instalador actualizado	
2.1.19	• Se ha agregado compatibilidad con el etiquetado de discos efímeros al utilizar el controlador de red Intel (por ejemplo, para el tipo de instancia C3). Para obtener más información, consulte Redes mejoradas en Amazon EC2. • Se ha agregado compatibilidad con la versión original de AMI y el nombre de origen de AMI para la salida de la consola • Se han realizado cambios en la salida de la consola para un formateo/análisis uniforme • Archivo de ayuda actualizado	

Versión	Detalles	Fecha de la versión
2.1.18	• Se ha añadido notificación de objeto para completar WMI EC2Config (-Namespace root\Amazon -Class EC2_ConfigService) • Se ha mejorado el rendimiento de las consultas WMI de inicio con registros de eventos grandes; podría provocar una alta demanda de CPU prolongada durante la ejecución inicial	
2.1.17	• Se ha corregido el problema de la ejecución de UserData al rellenar el búfer de salida estándar y error estándar • Se han corregido las huellas digitales de RDP incorrectas que aparecían a veces en la salida de la consola para >= SO w2k8 • La salida de la consola ahora contiene 'RDPCERTIFICATE-SubjectName:' para Windows 2008+, que contiene el valor del nombre de equipo • Se ha añadido D:\ al menú desplegable de mapeo de letras de unidad • Se ha movido el botón de ayuda a la parte superior derecha y se ha cambiado su aspecto/estilo • Se ha añadido un enlace para la encuesta de comentarios en la parte superior derecha	

Versión	Detalles	Fecha de la versión
2.1.16	• La pestaña general incluye un enlace a la página de descarga de EC2Config para nuevas versiones • La superposición del fondo de pantalla del escritorio ahora se almacena en la carpeta de datos de aplicación local del usuario en lugar de en Mis documentos para admitir el redireccionamiento a Mis documentos • Nombre de MSSQLServer sincronizado con el sistema en el script Post-Sysprep (2008+) • Se ha reorganizado la carpeta de aplicaciones (los archivos se han movido al directorio del complemento y los archivos duplicados se han eliminado) • Se ha cambiado el resultado del registro del sistema (consola) : • *Se ha pasado a un formato de fecha, nombre valor para un análisis más sencillo (comiencen a migrar las dependencias al nuevo formato) • *Se ha añadido el estado del complemento 'Ec2SetPassword' • *Se han añadido las horas de inicio de finalización: de Sysprep • Se ha corregido el problema por el que los discos efímeros no se etiquetaban como “almacenamiento temporal” en los sistemas operativos que no están en inglés • Se ha corregido el error de desinstalación de EC2Config tras ejecutar Sysprep	

Versión	Detalles	Fecha de la versión
2.1.15	• Solicitudes optimizadas al servicio de metadatos • Los metadatos ahora omiten los ajustes del proxy • Los discos efímeros etiquetados como “almacenamiento temporal” e Important.txt, colocados en el volumen cuando se localizan (solo controladores Citrix PV). Para obtener más información, consulte Actualizar controladores PV en instancias de Windows. • Los discos efímeros asignaban letras de unidad de la Z a la A (solo controladores Citrix PV) - esta asignación se puede se sobrescribir mediante el complemento de mapeo de letras de unidad con las etiquetas de volumen “Almacenamiento temporal X”, donde x es un número entre 0 y 25) • UserData ahora se ejecuta inmediatamente después de “Windows is Ready”	
2.1.14	Correcciones del fondo de pantalla del escritorio	
2.1.13	• El fondo de pantalla del escritorio mostrará el nombre de host de forma predeterminada • Se ha eliminado la dependencia del servicio horario de Windows • Se ha añadido una ruta en casos en los que se asignan varias IP a una misma interfaz	

Versión	Detalles	Fecha de la versión
2.1.11	• Re han realizado cambios en el complemento Ec2Activation • -Verifica el estado de la activación cada 30 días • -Si al periodo de gracia le quedan 90 días (de los 180), se vuelve a intentar la activación	
2.1.10	• La superposición del fondo de pantalla del escritorio ya no persiste con Sysprep ni se cierra sin Sysprep • Opción de ejecutar UserData en cada inicio de servicio con <persist>true</persist> • Se ha cambiado la ubicación y el nombre de /DisableWinUpdate.cmd a /Scripts/PostSysprep.cmd • Se establece la contraseña del administrador para que no caduque de forma predeterminada en /Scripts/PostSysprep.cmd • La desinstalación eliminará el script de PostSysprep de EC2Config de c:\windows\setup\script\CommandComplete.cmd • La opción de añadir ruta admite métricas de interfaz personalizadas	
2.1.9	La ejecución de UserData ya no está limitada a 3.851 caracteres	

Versión	Detalles	Fecha de la versión
2.1.7	• La versión del sistema operativo y el identificador de idioma se escriben en la consola • La versión de EC2Config se escribe en la consola • La versión del controlador PV se escribe en la consola • Detección de comprobación de errores y resultado a la consola durante el siguiente reinicio cuando se localizan • Se ha añadido la opción de que config.xml haga que persistan las credenciales de Sysprep • Lógica de reintento para la opción de añadir ruta en casos en los que la ENI no puede iniciarse • El PID de ejecución de los datos de usuario se escribe en la consola • La longitud mínima de la contraseña generada se extrae de GPO • El inicio del servicio se establece para que realice 3 intentos. • Se han añadido los ejemplos S3_DownloadFile.ps1 y S3_Upload file.ps1 a la carpeta /Scripts	

Versión	Detalles	Fecha de la versión
2.1.6	• Se ha añadido información de la versión a la pestaña General • Se ha cambiado el nombre de la pestaña Bundle por Image • Se ha simplificado el proceso de especificar contraseñas y se ha movido la interfaz de usuario relacionada con las contraseñas de la pestaña General a la pestaña Image • Se ha cambiado el nombre de la pestaña Disk Settings por Storage • Se ha añadido una pestaña Support con herramientas habituales para la solución de problemas • Se ha configurado `sysprep.ini` en Windows Server 2003 para que amplíe la partición del sistema operativo de forma predeterminada. • Se ha añadido la dirección IP privada al fondo de pantalla • La dirección IP privada se muestra en el fondo de pantalla • Se ha añadido lógica de reintento para la salida de la consola • Se ha corregido la excepción del puerto Com para la accesibilidad a los metadatos -- provocaba que EC2Config se terminase antes de que se mostrara la salida de la consola • Comprobación del estado de la activación en cada reinicio -- se activa según sea necesario • Se ha corregido el problema de las rutas relativas -- provocado al ejecutar manualmente el acceso directo al	

Versión	Detalles	Fecha de la versión
	fondo de pantalla desde la carpeta de inicio; apuntando hacia Administrador/logs • Se ha corregido el color de fondo predeterminado para usuarios de Windows Server 2003 (a excepción del administrador).	

Versión	Detalles	Fecha de la versión
2.1.2	• Marcas de tiempo de la consola en UTC (Zulú) • Se ha eliminado la aparición del hipervínculo en la pestaña Sysprep • Se ha añadido una opción para ampliar dinámicamente el volumen raíz en el primer arranque para Windows 2008+ • Cuando la opción de establecer contraseña está habilitad a, ahora permite que EC2Config establezca la contraseña automáticamente • EC2Config comprueba el estado de la activación antes de ejecutar Sysprep (muestra una advertencia si no está activado) • Ahora, `Sysprep.xml` en Windows Server 2003 establece de forma predeterminada la zona horaria UTC en lugar de la hora del Pacífico. • Servidores de activación aleatorios • Se ha cambiado el nombre de la pestaña Drive Mapping por Disk Settings • Se han movido los elementos de la interfaz de usuario para inicializar unidades de la pestaña General a la pestaña Disk Settings • El botón de ayuda ahora apunta hacia un archivo de ayuda HTML • Se ha actualizado el archivo de ayuda HTML con cambios •	

Versión	Detalles	Fecha de la versión
	Se ha actualizado el texto de notas para los mapeos de letras de unidad • Se ha añadido InstallUpdates.ps1 a la carpeta /Scripts para la automatización de parches y limpieza anteriores a Sysprep	
2.1.0	• El fondo de pantalla del escritorio muestra información sobre instancias de forma predeterminada durante el primer inicio de sesión (no se desconecta y se vuelve a conectar) • PowerShell se puede ejecutar a partir de UserData rodeando el código con <powershell></powershell>	

Suscribirse a las notificaciones del servicio EC2Config

Amazon SNS puede notificarle cuando se publiquen nuevas versiones del servicio EC2Config. Para suscribirse a estas notificaciones, utilice el siguiente procedimiento.

Para suscribirse a las notificaciones de EC2Config

1. Abra la consola de Amazon SNS en https://console.aws.amazon.com/sns/v3/home.
2. En la barra de navegación, cambie la región a EE. UU. Este (Norte de Virginia), si es necesario. Debe seleccionar esta región porque las notificaciones de SNS a las que se va a suscribir se han creado en esa región.
3. En el panel de navegación, seleccione Subscriptions.
4. Seleccione Create subscription.
5. En el cuadro de diálogo Create subscription (Crear suscripción), haga lo siguiente:
   a. En Topic ARN, use el siguiente nombre de recurso de Amazon (ARN):

      ```
      arn:aws:sns:us-east-1:801119661308:ec2-windows-ec2config
      ```

   b. En Protocol (Protocolo), elija `Email`.

c. En Punto de conexión, escriba una dirección de correo electrónico que pueda utilizar para recibir notificaciones.

d. Seleccione Create subscription.

6. Debe recibir un correo electrónico donde se solicita que confirme la suscripción. Abra el mensaje y siga las instrucciones para completar la suscripción.

Cada vez que se publique una nueva versión del servicio EC2Config, enviaremos una notificación a los suscriptores. Si ya no desea recibir estas notificaciones, utilice el siguiente procedimiento para cancelar la suscripción.

Para cancelar la suscripción a las notificaciones de EC2Config

1. Abra la consola de Amazon SNS.
2. En el panel de navegación, seleccione Subscriptions.
3. Seleccione la suscripción y, a continuación, elija Actions (Acciones), Delete subscriptions (Eliminar suscripciones). Cuando se le pida confirmación, seleccione Delete (Eliminar).

Solucionar problemas del servicio EC2Config

La siguiente información puede ayudarle a solucionar problemas del servicio EC2Config.

Actualizar EC2Config en una instancia inalcanzable

Utilice el procedimiento siguiente para actualizar el servicio EC2Config en una instancia de Windows Server que sea inalcanzable mediante el Escritorio remoto.

Para actualizar EC2Config en una instancia de Windows respaldada por Amazon EBS a la que no pueda conectarse

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancias).
3. Localice la instancia afectada. Selecciona la instancia, selecciona Estado de instanciay a continuación selecciona Detener instancia.

> ⚠ Warning
>
> Cuando detiene una instancia, se borran los datos contenidos en todos los volúmenes de almacén de instancias. Para conservar los datos de los volúmenes del almacén de

instancias, asegúrese de realizar una copia de seguridad de ellos en un almacenamiento persistente.

4. Selecciona iniciar instancias y crea una instancia `t2.micro` temporal en la misma zona de disponibilidad que la instancia afectada. Use una AMI diferente de la que haya empleado para iniciar la instancia afectada.

   > **Important**
   >
   > Si no crea la instancia en la misma zona de disponibilidad que la instancia afectada, no podrá adjuntar el volumen raíz de la instancia afectada a la nueva instancia.

5. En la consola de EC2, elija Volumes (Volúmenes).
6. Localice el volumen raíz de la instancia afectada. Desasocie el volumen y asócielo a la instancia temporal que ha creado antes. Adjúntelo con el nombre de dispositivo predeterminado (xvdf).
7. Utilice el Escritorio remoto para conectarse a la instancia temporal y, a continuación, utilice la utilidad de Administración de discos para hacer que el volumen esté disponible para su uso.
8. Descargue la última versión del servicio EC2Config. Extraiga los archivos del archivo `.zip` en el directorio `Temp` de la unidad que ha adjuntado.
9. En la instancia temporal, abra el cuadro de diálogo Ejecutar, escriba **`regedit`** y pulse Intro.
10. Elija `HKEY_LOCAL_MACHINE`. En el menú File (Archivo), elija Load Hive (Cargar Hive). Elija la unidad y, a continuación, navegue hasta ella y abra el siguiente archivo: `Windows \System32\config\SOFTWARE`. Cuando se le solicite, especifique un nombre de clave.
11. Seleccione la clave que acaba de cargar y navegue hasta `Microsoft\Windows \CurrentVersion`. Elija la clave `RunOnce`. Si esta clave no existe, elija `CurrentVersion` en el menú contextual (botón derecho), elija Nuevo y, a continuación, elija Clave. Asigne a la clave el nombre `RunOnce`.
12. En el menú contextual (botón derecho), elija la clave `RunOnce`, elija Nuevo y, a continuación, elija Valor de cadena. Escriba `Ec2Install` como nombre y `C:\Temp\Ec2Install.exe /quiet` como dato.
13. Elija la clave `HKEY_LOCAL_MACHINE\`*`specified key name`*`\Microsoft\Windows NT \CurrentVersion\Winlogon`. En el menú contextual (botón derecho), elija Nuevo y, a continuación, elija Valor de cadena. Escriba **`AutoAdminLogon`** como nombre y **`1`** como valor.
14. Elija la clave `HKEY_LOCAL_MACHINE\`*`specified key name`*`\Microsoft\Windows NT\CurrentVersion\Winlogon>`. En el menú contextual (botón derecho), elija Nuevo

y, a continuación, elija Valor de cadena. Escriba **`DefaultUserName`** como nombre y **`Administrator`** como valor.

15. Elija la clave `HKEY_LOCAL_MACHINE\`*`specified key name`*`\Microsoft\Windows NT\CurrentVersion\Winlogon`. En el menú contextual (botón derecho), elija Nuevo y, a continuación, elija Valor de cadena. Escriba **`DefaultPassword`** como nombre y escriba una contraseña en como valor.
16. En el panel de navegación del Editor del Registro, elija la clave temporal que creó cuando abrió el Editor del Registro por primera vez.
17. En el menú File (Archivo), elija Unload Hive (Descargar Hive).
18. En la utilidad de Administración de discos, elija la unidad que adjuntó anteriormente, abra el menú contextual (haga clic con el botón derecho) y, a continuación, elija Sin conexión.
19. En la consola de Amazon EC2, separe el volumen afectado de la instancia temporal y vuelva a adjuntarlo a la instancia con el nombre de dispositivo `/dev/sda1`. Debe especificar este nombre de dispositivo para designar el volumen como volumen raíz.
20. Detención e iniciación de una instancia de Amazon EC2 la instancia.
21. Una vez iniciada la instancia, compruebe el registro del sistema y verifique que puede ver el mensaje Windows is ready to use (Windows está listo para utilizarse).
22. Abra el Editor del Registro y elija `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon`. Elimine las claves de valores de cadena que creó anteriormente: AutoAdminLogon, DefaultUserName y DefaultPassword.
23. Elimine o detenga la instancia temporal que creó en este procedimiento.

Uso del lanzamiento rápido de EC2 para sus instancias de Windows

Todas las instancias de Amazon EC2 para Windows deben seguir los pasos de inicialización estándar del sistema operativo (SO) Windows, que incluyen varios reinicios y suelen tardar 15 minutos o más en completarse. Las AMI de Windows Server de Amazon EC2 que cuenten con la característica de lanzamiento rápido de EC2 habilitada completan algunos de esos pasos y reinicios por adelantado para reducir el tiempo de lanzamiento de una instancia.

Al configurar el lanzamiento rápido de EC2 de una AMI de Windows Server, Amazon EC2 crea un conjunto de instantáneas aprovisionadas previamente para que se utilicen para acelerar el lanzamiento, tal como se muestra a continuación.

1. Amazon EC2 inicia un conjunto de instancias t3 temporales, según su configuración.

2. A medida que cada instancia temporal completa los pasos de inicialización estándar, Amazon EC2 crea una instantánea aprovisionada previamente de la instancia. Almacena la instantánea en su bucket de Amazon S3.
3. Cuando la instantánea está lista, Amazon EC2 finaliza la instancia t3 asociada para mantener los costos de recursos lo más bajos posible.
4. La próxima vez que Amazon EC2 lanza una instancia desde una AMI con el lanzamiento rápido de EC2 habilitado, utiliza una instantánea para reducir de manera significativa el tiempo de lanzamiento.

Amazon EC2 repone de manera automática las instantáneas disponibles, ya que las utiliza para lanzar instancias desde la AMI con el lanzamiento rápido de EC2 habilitado.

Cualquier cuenta con acceso a una AMI con el lanzamiento rápido de EC2 habilitado puede aprovechar la reducción del tiempo de lanzamiento. Cuando el propietario de la AMI le concede acceso para iniciar instancias, las instantáneas aprovisionadas previamente provienen de la cuenta del propietario de la AMI.

Si se le comparte una AMI compatible con el lanzamiento rápido de EC2, usted puede habilitar o deshabilitar la función del lanzamiento rápido de la AMI compartida. Si habilita el lanzamiento rápido de EC2 en una AMI compartida, Amazon EC2 crea las instantáneas aprovisionadas previamente directamente en su cuenta. Si agota las instantáneas de su cuenta, podrá seguir utilizando las instantáneas de la cuenta del propietario de la AMI.

> **Note**
>
> El lanzamiento rápido de EC2 elimina las instantáneas aprovisionadas previamente en el momento en que se consumen en un lanzamiento para disminuir los costos de almacenamiento y evitar la reutilización. Sin embargo, si las instantáneas eliminadas cumplen una regla de retención, la Papelera de reciclaje las conserva automáticamente. Le recomendamos que revise el alcance de las reglas de retención de la Papelera de reciclaje para que esto no suceda. Para obtener más información, consulte Consideraciones.
> Esta característica no es la misma que la restauración rápida de instantáneas de EBS. Debe habilitar la restauración rápida de instantáneas de EBS de forma explícita para cada instantánea y tiene sus propios costos asociados.

En el siguiente video, se muestra cómo configurar la AMI de Windows para un inicio más rápido con una descripción general rápida de los términos clave relacionados y sus definiciones: inicialización de instancias de EC2 para Windows hasta un 65 % más rápido en AWS.

Costos de recursos

La configuración del lanzamiento rápido de EC2 en las AMI de Windows no incurren en ningún cargo de servicio. Sin embargo, se aplica un precio estándar a cualquier recurso de AWS subyacente que utiliza Amazon EC2. Para obtener más información sobre los costos de los recursos asociados y cómo administrarlos, consulte Administración de los costos de los recursos con el lanzamiento rápido de EC2.

Contenidos

Términos clave

La característica de lanzamiento rápido de EC2 utiliza los siguientes términos clave:

Instantánea aprovisionada previamente

Una instantánea de una instancia lanzada desde una AMI de Windows con el lanzamiento rápido de EC2 habilitado, que completó los pasos de lanzamiento de Windows y se reinició según lo requerido.

- Especialización de Sysprep
- Configuración rápida (OOBE) de Windows

Una vez que se completan los pasos, el lanzamiento rápido de EC2 detiene la instancia y crea una instantánea que se utilizará más adelante para un lanzamiento rápido desde la AMI, según la configuración.

Frecuencia de inicialización

Controla el número de instantáneas aprovisionadas previamente que Amazon EC2 puede iniciar durante el periodo especificado. Cuando se habilita el lanzamiento rápido de EC2 para una AMI, Amazon EC2 crea el conjunto inicial de instantáneas aprovisionadas previamente en segundo plano. Por ejemplo, si la frecuencia de lanzamiento se configura en cinco lanzamientos por hora, que es la frecuencia predeterminada, el lanzamiento rápido de EC2 crea un conjunto inicial de cinco instantáneas aprovisionadas previamente.

Cuando Amazon EC2 lanza una instancia desde una AMI con el lanzamiento rápido de EC2 habilitado, utiliza una de las instantáneas aprovisionadas previamente para reducir el tiempo de lanzamiento. A medida que se consumen instantáneas, se van reponiendo automáticamente, hasta llegar al número especificado por la frecuencia de inicialización.

Si espera un pico en el número de instancias que se inician desde la AMI (por ejemplo, durante un evento especial), puede aumentar la frecuencia de inicialización de antemano para cubrir las instancias adicionales que necesitará. Cuando el ritmo de inicializaciones vuelva a la normalidad, se puede ajustar la frecuencia a la baja.

Cuando necesite realizar un número de inicializaciones superior al previsto, puede utilizar las instantáneas aprovisionadas previamente que tenga disponibles. Esto no genera errores de inicialización. Sin embargo, puede dar lugar a que algunas instancias pasen por el proceso de inicialización estándar, hasta que se puedan reabastecer las instantáneas.

Número de recursos de destino

El número de instantáneas aprovisionadas previamente que deben estar disponibles para una AMI de Windows Server de Amazon EC2 con el lanzamiento rápido de EC2 habilitado.

Número máximo de inicializaciones en paralelo

Controla la cantidad de instancias que Amazon EC2 puede lanzar en simultáneo para crear instantáneas aprovisionadas previamente para el lanzamiento rápido de EC2. Si el recuento de recursos de destino es superior al número máximo de inicializaciones en paralelo que ha configurado, Amazon EC2 inicia inicialmente el número de instancias especificado por la configuración Número máximo de inicializaciones en paralelo para comenzar a crear las instantáneas. A medida que esas instancias completan el proceso, Amazon EC2 toma la instantánea y detiene la instancia. Luego, continúa la inicialización de más instancias hasta que el número total de instantáneas disponibles haya alcanzado el número de recursos de destino. El valor de Número máximo de inicializaciones en paralelo debe ser de 6 o más.

Requisitos previos del lanzamiento rápido de EC2

Antes de configurar el lanzamiento rápido de EC2, verifique que cumpla con los siguientes requisitos necesarios para crear las instantáneas para las AMI en su Cuenta de AWS:

- Si no utiliza una plantilla de lanzamiento para la configuración, asegúrese de que haya una VPC predeterminada configurada para la región en la utilice el lanzamiento rápido de EC2.

  > **Note**
  >
  > Si por accidente elimina la VPC predeterminada en la región en donde planea utilizar el lanzamiento rápido de EC2, puede crear una nueva VPC predeterminada en esa región. Para obtener más información, consulte Creación de una VPC predeterminada en la Guía de usuario de Amazon VPC.

- Para especificar una VPC no predeterminada, debe usar una plantilla de inicialización cuando configure el inicio rápido de Windows. Para obtener más información, consulte Utilice una plantilla de lanzamiento al momento de configurar un lanzamiento rápido de EC2.
- Si la cuenta incluye una política que aplica IMDSv2 a las instancias de Amazon EC2, debe crear una plantilla de inicialización que especifique la configuración de metadatos para aplicar IMDSv2.
- Las AMI privadas con lanzamiento rápido de EC2 deben ser compatibles con la ejecución de scripts de datos de usuario.
- Para configurar el lanzamiento rápido de EC2 para una AMI, debe utilizar Sysprep para crear la AMI con la opción de cierre. En la actualidad, la característica de lanzamiento rápido de EC2 no es compatible con las AMI creadas a partir de una instancia en ejecución.

  Para crear una AMI mediante Sysprep, consulte Creación de una AMI con Windows Sysprep.
- La cuota predeterminada para Número máximo de inicializaciones en paralelo en todas las AMI de una Cuenta de AWS es de 40 por región. Puede solicitar un aumento de Service Quotas para su cuenta de la siguiente manera.

  1. Inicie sesión en la AWS Management Console y abra la consola de Service Quotas en https://console.aws.amazon.com/servicequotas/.
  2. En el panel de navegación, elija Servicios de AWS.
  3. En la barra de búsqueda, ingrese `EC2 Fast Launch` y seleccione el resultado.
  4. Seleccione el enlace de `Parallel instance launches`. Esto lo lleva a la página de detalles de Service Quotas para inicializaciones de instancias en paralelo.

5. Elija Solicitar aumento de cuota.

Para obtener más información, consulte Solicitud de un aumento de cuota en la Guía del usuario de Service Quotas.

Configure la configuración del lanzamiento rápido de EC2 para la AMI de Windows Server de Amazon EC2

Puede configurar el lanzamiento rápido de EC2 de las AMI de Windows propias o de las AMI compartidas desde la AWS Management Console, la API, los SDK, CloudFormation o la AWS Command Line Interface (AWS CLI). Antes de configurar el lanzamiento rápido de EC2, verifique que la AMI cumpla con los requisitos necesarios para crear las instantáneas aprovisionadas previamente. Para obtener más información, consulte Requisitos previos del lanzamiento rápido de EC2.

Las siguientes secciones tratan sobre los pasos de configuración de la consola de Amazon EC2 y la AWS CLI.

Habilite el lanzamiento rápido de EC2

Para habilitar el lanzamiento rápido de EC2, seleccione la pestaña compatible con el entorno y siga los pasos.

> **Note**
>
> Antes de cambiar esta configuración, asegúrese de que la AMI y la región en la que se ejecuta cumplan todos los Requisitos previos del lanzamiento rápido de EC2.

Console

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Imágenes, elija AMI.
3. Elija la AMI que desea actualizar mediante la selección de la casilla de verificación situada junto al Nombre.
4. En el menú Acciones situado encima de la lista de AMI, elija Configurar el inicio rápido. Esto abrirá la página Configurar el lanzamiento rápido, en donde puede configurar el lanzamiento rápido de EC2.

5. Para empezar a utilizar instantáneas aprovisionadas previamente a fin de iniciar instancias desde la AMI de Windows más rápido, seleccione la casilla Habilitar el inicio rápido de Windows.
6. En la lista desplegable Establecer la frecuencia de inicialización prevista, elija un valor para especificar el número de instantáneas que desea crear y mantener para cubrir el volumen de inicialización de instancias esperado.
7. Cuando termine de realizar los cambios, elija Guardar Cambios.

> **Note**
>
> Si necesita utilizar una plantilla de inicialización para especificar una VPC no predeterminada o para configurar la configuración de metadatos de IMDSv2, consulte Utilice una plantilla de lanzamiento al momento de configurar un lanzamiento rápido de EC2.

AWS CLI

El comando enable-fast-launch llama a la operación de la API EnableFastLaunch de Amazon EC2.

Sintaxis:

```
aws ec2 enable-fast-launch \
  --image-id <value> \
  --resource-type <value> \ (optional)
  --snapshot-configuration <value> \ (optional)
  --launch-template <value> \ (optional)
  --max-parallel-launches <value> \ (optional)
  --dry-run | --no-dry-run \  (optional)
  --cli-input-json <value> \ (optional)
  --generate-cli-skeleton <value> \ (optional)
```

Ejemplo:

En el siguiente ejemplo de enable-fast-launch, se habilita el lanzamiento rápido de EC2 para una AMI específica y se lanzan seis instancias en simultáneo para el aprovisionamiento previo. `ResourceType` está establecido como `snapshot`, el valor predeterminado.

```
aws ec2 enable-fast-launch \
         --image-id ami-01234567890abcedf  \
         --max-parallel-launches 6 \
         --resource-type snapshot
```

Salida:

```
{
     "ImageId": "ami-01234567890abcedf",
     "ResourceType": "snapshot",
     "SnapshotConfiguration": {
         "TargetResourceCount": 10
     },
     "LaunchTemplate": {},
     "MaxParallelLaunches": 6,
     "OwnerId": "0123456789123",
     "State": "enabling",
     "StateTransitionReason": "Client.UserInitiated",
     "StateTransitionTime": "2022-01-27T22:16:03.199000+00:00"
 }
```

Tools for PowerShell

El cmdlet Enable-EC2FastLaunch llama a la operación de la API EnableFastLaunch de Amazon EC2 para habilitar el lanzamiento rápido de EC2 en la AMI de Windows.

Sintaxis:

```
Enable-EC2FastLaunch
      -ImageId <String>
      -LaunchTemplate_LaunchTemplateId <String>
      -LaunchTemplate_LaunchTemplateName <String>
      -MaxParallelLaunch <Int32>
      -ResourceType <String>
      -SnapshotConfiguration_TargetResourceCount <Int32>
      -LaunchTemplate_Version <String>
      -Select <String>
      -PassThru <SwitchParameter>
      -Force <SwitchParameter>
```

Ejemplo:

En el siguiente ejemplo de Enable-EC2FastLaunch, se habilita el lanzamiento rápido de EC2 para una AMI específica y se lanzan seis instancias en simultáneo para el aprovisionamiento previo. `ResourceType` está establecido como `snapshot`, el valor predeterminado.

```
Enable-EC2FastLaunch `
 -ImageId ami-01234567890abcedf `
 -MaxParallelLaunch 6 `
 -Region us-west-2 `
 -ResourceType snapshot
```

Salida:

```
ImageId               : ami-01234567890abcedf
LaunchTemplate        :
MaxParallelLaunches   : 6
OwnerId               : 0123456789123
ResourceType          : snapshot
SnapshotConfiguration : Amazon.EC2.Model.FastLaunchSnapshotConfigurationResponse
State                 : enabling
StateTransitionReason : Client.UserInitiated
StateTransitionTime   : 2/25/2022 12:24:11 PM
```

Deshabilite el lanzamiento rápido de EC2

Para deshabilitar el lanzamiento rápido de EC2, seleccione la pestaña compatible con el entorno y siga los pasos.

> **Note**
>
> Antes de cambiar esta configuración, asegúrese de que la AMI y la región en la que se ejecuta cumplan todos los Requisitos previos del lanzamiento rápido de EC2.

Console

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Imágenes, elija AMI.

3. Elija la AMI que desea actualizar mediante la selección de la casilla de verificación situada junto al Nombre.
4. En el menú Acciones situado encima de la lista de AMI, elija Configurar el inicio rápido. Esto abrirá la página Configurar el lanzamiento rápido, en donde puede configurar el lanzamiento rápido de EC2.
5. Quite la selección de la casilla Habilitar el lanzamiento rápido para Windows para deshabilitar el lanzamiento rápido de EC2 y eliminar las instantáneas aprovisionadas previamente. Esto da como resultado que, en el futuro, la AMI utilice el proceso de inicialización estándar para cada instancia.

   > **Note**
   >
   > Al deshabilitar la optimización de imágenes de Windows, las instantáneas existentes aprovisionadas previamente se eliminan de forma automática. Se debe completar este paso antes de poder volver a utilizar la característica.

6. Cuando termine de realizar los cambios, elija Save (Guardar).

AWS CLI

El comando disable-fast-launch llama a la operación de la API DisableFastLaunch de Amazon EC2.

Sintaxis:

```
aws ec2 disable-fast-launch \
  --image-id <value> \
  --force | --no-force \ (optional)
  --dry-run | --no-dry-run \ (optional)
  --cli-input-json <value> \ (optional)
  --generate-cli-skeleton <value> \ (optional)
```

Ejemplo:

En el siguiente ejemplo de disable-fast-launch, se deshabilita el lanzamiento rápido de EC2 para una AMI específica y elimina las instantáneas aprovisionadas previamente existentes.

```
aws ec2 disable-fast-launch \
         --image-id ami-01234567890abcedf
```

Salida:

```
{
     "ImageId": "ami-01234567890abcedf",
     "ResourceType": "snapshot",
     "SnapshotConfiguration": {},
     "LaunchTemplate": {
         "LaunchTemplateId": "lt-01234567890abcedf",
         "LaunchTemplateName": "EC2FastLaunchDefaultResourceCreation-
a8c6215d-94e6-441b-9272-dbd1f87b07e2",
         "Version": "1"
     },
     "MaxParallelLaunches": 6,
     "OwnerId": "0123456789123",
     "State": "disabling",
     "StateTransitionReason": "Client.UserInitiated",
     "StateTransitionTime": "2022-01-27T22:47:29.265000+00:00"
 }
```

Tools for PowerShell

El cmdlet Disable-EC2FastLaunch llama a la operación de la API DisableFastLaunch de Amazon EC2.

Sintaxis:

```
Disable-EC2FastLaunch
      -ImageId <String>
      -ForceStop <Boolean>
      -Select <String>
      -PassThru <SwitchParameter>
      -Force <SwitchParameter>
```

Ejemplo:

En el siguiente ejemplo de disable-EC2fastlaunch, se deshabilita el lanzamiento rápido de EC2 para una AMI específica y elimina las instantáneas aprovisionadas previamente existentes.

```
Disable-EC2FastLaunch -ImageId ami-01234567890abcedf
```

Salida:

```
ImageId               : ami-01234567890abcedf
LaunchTemplate        :
Amazon.EC2.Model.FastLaunchLaunchTemplateSpecificationResponse
MaxParallelLaunches   : 6
OwnerId               : 0123456789123
ResourceType          : snapshot
SnapshotConfiguration :
State                 : disabling
StateTransitionReason : Client.UserInitiated
StateTransitionTime   : 2/25/2022 1:10:08 PM
```

Utilice una plantilla de lanzamiento al momento de configurar un lanzamiento rápido de EC2

Con una plantilla de inicialización, puede configurar un conjunto de parámetros de inicialización que Amazon EC2 utiliza cada vez que inicia una instancia desde esa plantilla. Puede especificar cosas como una AMI para usarla en la imagen base, los tipos de instancias, el almacenamiento, la configuración de red y más.

Las plantillas de inicialización son opcionales, excepto en los siguientes casos específicos, en los que debe usar una plantilla de inicialización para la AMI de Windows cuando configure un inicialización más rápido:

- Debe utilizar una plantilla de inicialización para especificar una VPC no predeterminada para la AMI de Windows.
- Si la cuenta incluye una política que aplica IMDSv2 a las instancias de Amazon EC2, debe crear una plantilla de inicialización que especifique la configuración de metadatos para aplicar IMDSv2.

  Utilice la plantilla de inicialización que incluye la configuración de sus metadatos desde la consola de EC2, o cuando ejecute el comando enable-fast-launch en la AWS CLI, o bien llame a la acción de la API EnableFastLaunch.

El lanzamiento rápido de EC2 de Amazon EC2 no es compatible con las siguientes configuraciones al momento de utilizar una plantilla de lanzamiento. Si utiliza una plantilla de lanzamiento para el lanzamiento rápido de EC2, no debe especificar nada de lo que se menciona a continuación:

- Datos de usuario
- Protección de terminación

- Metadatos
- Opción de spot
- Comportamiento de cierre que termina la instancia
- Etiquetas de recursos para solicitudes de interfaz de red, gráficos elásticos o instancias de spot puntuales

Especificar una VPC no predeterminada

Paso 1: crear una plantilla de inicialización

Cree una plantilla de inicialización que especifique los siguientes detalles para sus instancias de Windows:

- La subred de VPC.
- Un tipo de instancia `t3.xlarge`.

Para obtener más información, consulte Creación de una plantilla de lanzamiento.

Paso 2: Especifique la plantilla de lanzamiento para la AMI con lanzamiento rápido de EC2

Elija la pestaña que coincida con su proceso:

Console

Para especificar la plantilla de lanzamiento para el lanzamiento rápido de EC2 desde la AWS Management Console, siga estos pasos:

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Imágenes, elija AMI.
3. Elija la AMI que desea actualizar mediante la selección de la casilla de verificación situada junto al Nombre.
4. En el menú Acciones situado encima de la lista de AMI, elija Configurar el inicio rápido. Esto abrirá la página Configurar el lanzamiento rápido, en donde puede configurar el lanzamiento rápido de EC2.
5. La caja Plantilla de inicialización realiza una búsqueda filtrada que encuentra plantillas de inicialización en su cuenta dentro la región actual y que coinciden con el texto que ha ingresado. Especifique todo o parte del nombre o ID de la plantilla de inicialización en el cuadro para mostrar una lista de plantillas de inicialización coincidentes. Por ejemplo, si

especifica `fast` en el cuadro, Amazon EC2 encuentra todas las plantillas de inicialización de su cuenta en la región actual que tienen “fast” (rápido) en el nombre.

Para crear una nueva plantilla de inicialización, elija Crear plantilla de inicialización.

6. Al seleccionar una plantilla de inicialización, Amazon EC2 muestra la versión predeterminada de esa plantilla en la caja Versión de plantilla de origen. Para especificar una versión diferente, resalte la versión predeterminada para sustituirla y especifique el número de versión que desee en el cuadro.
7. Cuando termine de realizar los cambios, elija Guardar.

AWS CLI, API

Para especificar la plantilla de lanzamiento del lanzamiento rápido de EC2 desde la AWS CLI, especifique el nombre de la plantilla de lanzamiento o el ID en el parámetro `--launch-template` al momento de ejecutar el comando enable-fast-lauch en la AWS CLI.

Para especificar la plantilla de lanzamiento del lanzamiento rápido de EC2 en una solicitud de API, especifique el nombre de la plantilla de lanzamiento o el ID en el parámetro `LaunchTemplate` al momento de realizar la llamada a la API EnableFastLauch.

Para obtener más información acerca de las plantillas de inicialización de EC2, consulte iniciar una instancia desde una plantilla de inicialización.

Cree una imagen personalizada con el lanzamiento rápido de EC2 habilitado

El lanzamiento rápido de EC2 de Amazon EC2 se integra con el Generador de imágenes de EC2 para ayudar a crear imágenes personalizadas con el lanzamiento rápido de EC2 habilitado. Para obtener más información, consulte Crear una configuración de distribución para una AMI de Windows con inicio rápido de EC2 habilitado (AWS CLI) en la Guía del usuario del Generador de imágenes de EC2.

Visualización de las AMI con lanzamiento rápido de EC2 habilitado

Puede utilizar el comando describe-fast-launch-images en AWS CLI o el Cmdlet Get-EC2FastLaunchImage de herramientas para PowerShell para obtener detalles de las AMI que cuentan con el lanzamiento rápido de EC2 habilitado.

Amazon EC2 proporciona los siguientes detalles para cada AMI de Windows que aparecerán en los resultados de búsqueda:

- El ID de imagen de una AMI con el lanzamiento rápido de EC2 habilitado.
- El tipo de recurso que se utiliza para el aprovisionamiento previo de la AMI de Windows asociada. Valor compatible: `snapshot`.
- La configuración de las instantáneas, que es un grupo de parámetros que configuran el aprovisionamiento previo para la AMI de Windows asociada mediante instantáneas.
- La información de la plantilla de inicialización, incluido el ID, el nombre y la versión de la plantilla de inicialización que utiliza la AMI asociada cuando inicia instancias de Windows desde instantáneas aprovisionadas previamente.
- El número máximo de instancias que se pueden iniciar al mismo tiempo para crear recursos.
- El ID del propietario de la AMI asociada. No se rellena para las AMI que se compartieron con usted.
- El estado actual del lanzamiento rápido de EC2 para la AMI asociada. Los valores compatibles incluyen: `enabling | enabling-failed | enabled | enabled-failed | disabling | disabling-failed`.

> **Note**
>
> También puede ver el estado actual, que se muestra en la página Administrar optimización de imágenes de la consola de EC2, como Estado de optimización de imágenes.

- La razón por la cual el lanzamiento rápido de EC2 para la AMI asociada cambió al estado actual.
- La hora en que el lanzamiento rápido de EC2 para la AMI asociada cambió al estado actual.

Elija la pestaña que corresponda al entorno de línea de comandos:

AWS CLI

El comando describe-fast-launch-images llama a la operación de la API DescribeFastLaunchImages de Amazon EC2.

Sintaxis:

```
aws ec2 describe-fast-launch-images \
 --image-ids <value> \ (optional)
 --filters <value> \ (optional)
 --dry-run | --no-dry-run \ (optional)
 --cli-input-json <value> \ (optional)
```

```
 --starting-token <value> \ (optional)
 --page-size <value> \ (optional)
 --max-items <value> \ (optional)
 --generate-cli-skeleton <value> \ (optional)
```

Ejemplo:

En el siguiente ejemplo de describe-fast-launch-images, se describen los detalles de cada AMI en la cuenta que esté configurada con el lanzamiento rápido de EC2. En este ejemplo, solo hay una AMI con el lanzamiento rápido de EC2 en la cuenta.

```
aws ec2 describe-fast-launch-images
```

Salida:

```
{
    "FastLaunchImages": [
        {
            "ImageId": "ami-01234567890abcedf",
            "ResourceType": "snapshot",
            "SnapshotConfiguration": {},
            "LaunchTemplate": {
                "LaunchTemplateId": "lt-01234567890abcedf",
                "LaunchTemplateName": "EC2FastLaunchDefaultResourceCreation-
a8c6215d-94e6-441b-9272-dbd1f87b07e2",
                "Version": "1"
            },
            "MaxParallelLaunches": 6,
            "OwnerId": "0123456789123",
            "State": "enabled",
            "StateTransitionReason": "Client.UserInitiated",
            "StateTransitionTime": "2022-01-27T22:20:06.552000+00:00"
        }
    ]
}
```

Tools for PowerShell

El cmdlet Get-EC2FastLaunchImage llama a la operación de la API DescribeFastLaunchImages de Amazon EC2.

Sintaxis:

```
Get-EC2FastLaunchImage
-Filter <Filter[]>
-ImageId <String[]>
-MaxResult <Int32>
-NextToken <String>
-Select <String>
-NoAutoIteration <SwitchParameter>
```

Ejemplo:

En el siguiente ejemplo de Get-EC2FastLaunchImage, se describen los detalles de cada AMI en la cuenta que esté configurada con el lanzamiento rápido de EC2. En este ejemplo, solo hay una AMI con el lanzamiento rápido de EC2 en la cuenta.

```
Get-EC2FastLaunchImage -ImageId ami-01234567890abcedf
```

Salida:

```
ImageId               : ami-01234567890abcedf
LaunchTemplate        :
 Amazon.EC2.Model.FastLaunchLaunchTemplateSpecificationResponse
MaxParallelLaunches   : 6
OwnerId               : 0123456789123
ResourceType          : snapshot
SnapshotConfiguration :
State                 : enabled
StateTransitionReason : Client.UserInitiated
StateTransitionTime   : 2/25/2022 12:54:43 PM
```

Administración de los costos de los recursos con el lanzamiento rápido de EC2

La configuración del lanzamiento rápido de EC2 en las AMI de Windows no incurren en ningún cargo de servicio. Sin embargo, al habilitar el lanzamiento rápido de EC2 para AMI de Windows de Amazon EC2 se aplica el precio estándar para los recursos de AWS subyacentes que utiliza Amazon EC2 para preparar y almacenar las instantáneas aprovisionadas previamente. Puede configurar las etiquetas de asignación de costos para ayudarlo a controlar y administrar los costos asociados con los recursos del lanzamiento rápido de EC2. Para obtener más información acerca de cómo

configurar las etiquetas de asignación de costos, consulte Controle los costos del lanzamiento rápido de EC2 en su factura.

En el siguiente ejemplo, se demuestra cómo se pueden asignar los costos asociados con las instantáneas del lanzamiento rápido de EC2.

Escenario de ejemplo: la compañía AtoZ Example tiene una AMI de Windows con un volumen raíz de EBS de 50 GiB. Habilitan el lanzamiento rápido de EC2 para su AMI y establecen el recuento de recursos en cinco. En el transcurso de un mes, el costo de utilización del lanzamiento rápido de EC2 para sus AMI es de, aproximadamente, 5,00 USD y se puede desglosar de la siguiente manera:

1. Cuando AtoZ Example habilita el lanzamiento rápido de EC2, Amazon EC2 lanza cinco instancias pequeñas. Cada instancia sigue los pasos de inicialización de Sysprep y OOBE de Windows y se reinicia según lo requerido. Se necesitan varios minutos para cada instancia (el tiempo puede variar, en función de la ocupación de la región o zona de disponibilidad [AZ] y del tamaño de la AMI).

   Costos

   - Costos de tiempo de ejecución de instancias (o tiempo de ejecución mínimo, si procede): cinco instancias
   - Costos de volumen: cinco volúmenes raíz de EBS

2. Cuando concluye el proceso de aprovisionamiento previo, Amazon EC2 toma una instantánea de la instancia, que almacena en Amazon S3. Por lo general, las instantáneas se almacenan entre 4 y 8 horas antes de ser consumidas por un inicialización. En este caso, el costo es aproximadamente entre 0,02 USD y 0,05 USD por instantánea.

   Costos

   - Almacenamiento de instantáneas (Amazon S3): cinco instantáneas

3. Cuando Amazon EC2 toma la instantánea, detiene la instancia. En ese momento, la instancia deja de generar costos. No obstante, siguen generándose costos por los volúmenes de EBS.

   Costos

   - Volúmenes de EBS: los volúmenes raíz de EBS asociados siguen generando costos.

> **Note**
>
> Los costos que se muestran aquí solo tienen fines ilustrativos. Los costos reales variarán, en función de la configuración de su AMI y del plan de precios.

Controle los costos del lanzamiento rápido de EC2 en su factura

Las etiquetas de asignación de costos pueden ayudar a configurar que la factura de AWS refleje los costos asociados con el lanzamiento rápido de EC2. Puede utilizar la siguiente etiqueta que Amazon EC2 agrega a los recursos que crea al preparar y almacenar las instantáneas aprovisionadas previamente para el lanzamiento rápido de EC2:

Clave de etiqueta: `CreatedBy`, Valor: `EC2 Fast Launch`

Tras activar la etiqueta en la consola de administración de facturación y costos y configurar el informe de facturación detallado, la columna `user:CreatedBy` aparece en el informe. En la columna se incluyen los valores de todos los servicios. Sin embargo, si descarga el archivo CSV, puede importar los datos a una hoja de cálculo y filtrar por `EC2 Fast Launch` en el valor. Esta información también aparece en el AWS Cost and Usage Report cuando la etiqueta está activada.

Paso 1: activar las etiquetas de asignación de costos definidas por el usuario

Para incluir etiquetas de recursos en los informes de costos, primero debe activar la etiqueta en la consola de administración de facturación y costos. Para obtener más información, consulte Activación de etiquetas de asignación de costos definidas por el usuario en la Guía del usuario AWS Billing and Cost Management.

> **Note**
>
> La activación puede tardar hasta 24 horas.

Paso 2: configurar un informe de costos

Si ya ha configurado un informe de costos, aparecerá una columna para la etiqueta la próxima vez que se ejecute el informe una vez completada la activación. Para configurar los informes de costos por primera vez, elija una de las siguientes opciones.

- Consulte Configuración de un informe de asignación de costos mensual en la Guía del usuario de AWS Billing and Cost Management.
- Consulte Creación de reportes de costo y uso en la Guía del usuario AWS Cost and Usage Report.

> **Note**
>
> AWS puede tardar hasta 24 horas en comenzar a entregar informes a su bucket S3.

Puede configurar el lanzamiento rápido de EC2 de las AMI de Windows propias o de las AMI compartidas desde la consola de Amazon EC2, la API, los SDK, CloudFormation o los comandos de ec2 en la AWS CLI. Las siguientes secciones tratan sobre los pasos de configuración de la consola de Amazon EC2 y la AWS CLI.

También puede crear AMI de Windows personalizadas con la configuración de lanzamiento rápido de EC2 con el Generador de imágenes de EC2. Para más información, consulte Creación de configuraciones de distribución para una AMI de Windows con el lanzamiento rápido de EC2 habilitado (AWS CLI).

Supervise el lanzamiento rápido de EC2

En esta sección, se explica cómo supervisar las AMI de Windows Server de Amazon EC2 de su cuenta que cuentan con el lanzamiento rápido de EC2 habilitado.

Supervise los cambios de estado del lanzamiento rápido de EC2 con EventBridge

Cuando hay un cambio de estado de una AMI de Windows con el lanzamiento rápido de EC2 habilitado, Amazon EC2 genera el evento `EC2 Fast Launch State-change Notification`. A continuación, Amazon EC2 envía el evento de cambio de estado a Amazon EventBridge (antes conocido como Eventos de Amazon CloudWatch).

Puede crear reglas de EventBridge que activen una o más acciones en respuesta al evento de cambio de estado. Por ejemplo, puede crear una regla de EventBridge que detecte el momento en que se habilite el lanzamiento rápido de EC2 y que realice las siguientes acciones:

- Envíe un mensaje a un tema de Amazon SNS que notifique a sus suscriptores.
- Invoca una función de Lambda que realice alguna acción.
- Envía los datos del cambio de estado a Amazon Data Firehose para su análisis.

Para obtener más información, consulte Creación de reglas de EventBridge que reaccionan a eventos en la Guía del usuario de Amazon EventBridge.

Eventos de cambio de estado

La característica de lanzamiento rápido de EC2 emite eventos de cambio de estado en formato JSON sobre la base del mejor esfuerzo. Amazon EC2 envía los eventos a EventBridge en tiempo casi real. En esta sección se describen los campos de eventos y se muestra un ejemplo del formato del evento.

`EC2 Fast Launch State-change Notification`

imageId

Identifica la AMI cuyo estado de lanzamiento rápido de EC2 cambió.

resourceType

El tipo de recurso que se utilizará para el aprovisionamiento previo. Valor compatible: `snapshot`. El valor predeterminado es `snapshot`.

estado

El estado actual de la característica de lanzamiento rápido de EC2 para la AMI especificada. Entre los valores válidos se incluyen los siguientes:

- enabling: habilitó la característica de lanzamiento rápido de EC2 para la AMI y Amazon EC2 comenzó a crear instantáneas para los procesos aprovisionados previamente.
- enabling-failed: se produjo un error que causó que el proceso de aprovisionamiento previo falle la primera vez que se habilitó el lanzamiento rápido de EC2 para una AMI. Esto puede ocurrir en cualquier momento durante el proceso de aprovisionamiento previo.
- enabled: la característica de lanzamiento rápido de EC2 está habilitada. El estado cambia a `enabled` el momento en que Amazon EC2 crea la primera instantánea aprovisionada previamente para cada nueva AMI con lanzamiento rápido de EC2. Si la AMI ya estaba habilitada y vuelve a pasar por el aprovisionamiento previo, el cambio de estado se produce de inmediato.
- enabled-failed: este estado solo es posible si no es la primera vez que la AMI con lanzamiento rápido de EC2 atraviesa un proceso de aprovisionamiento previo. Esto puede suceder si la característica de lanzamiento rápido de EC2 se deshabilita y luego se habilita nuevamente o si hay un cambio en la configuración y otro error luego de que se completa el aprovisionamiento previo por primera vez.

- disabling: el propietario de la AMI deshabilitó la característica de lanzamiento rápido de EC2 para la AMI y Amazon EC2 comenzó con el proceso de eliminación.
- disabled: la característica de lanzamiento rápido de EC2 está deshabilitada. El estado cambia a `disabled` tan pronto como Amazon EC2 complete el proceso de limpieza.
- disabling-failed: se produjo un error que provocó un error en el proceso de limpieza. Esto significa que es posible que algunas instantáneas aprovisionadas previamente aún permanezcan en la cuenta.

stateTransitionReason

La razón por la cual el estado cambió para la AMI de lanzamiento rápido de EC2.

> **Note**
>
> Todos los campos de este mensaje de evento son obligatorios.

El siguiente ejemplo muestra una AMI con el lanzamiento rápido de EC2 recién habilitado y que ha lanzado la primera instancia para iniciar el proceso de aprovisionamiento previo. En este punto, el estado es `enabling`. Una vez que Amazon EC2 crea la primera instantánea aprovisionada previamente, el estado cambia a `enabled`.

```
{
 "version": "0",
 "id": "01234567-0123-0123-0123-012345678901",
 "detail-type": "EC2 Fast Launch State-change Notification",
 "source": "aws.ec2",
 "account": "123456789012",
 "time": "2022-08-31T20:30:12Z",
 "region": "us-east-1",
 "resources": [
  "arn:aws:ec2:us-east-1:123456789012:image/ami-123456789012"
 ],
 "detail": {
  "imageId": "ami-123456789012",
  "resourceType": "snapshot",
  "state": "enabling",
  "stateTransitionReason": "Client.UserInitiated"
 }
}
```

Supervise las métricas del lanzamiento rápido de EC2 con CloudWatch

Las AMI de Amazon EC2 con el lanzamiento rápido de EC2 habilitado envían métricas a Amazon CloudWatch. Puede utilizar la AWS Management Console, la AWS CLI o una API para acceder a la lista de las métricas que el lanzamiento rápido de EC2 envía a CloudWatch. El espacio de nombres de `AWS/EC2` incluye las siguientes métricas del lanzamiento rápido de EC2:

Métrica	Descripción
NumberOfAvailableFastLaunchSnapshots	La cantidad de instantáneas aprovisionadas previamente disponibles por cada AMI con el lanzamiento rápido de EC2 habilitado.
NumberOfInstancesFastLaunched	La cantidad de instancias por cada AMI con el lanzamiento rápido de EC2 habilitado que se lanzaron a partir de instantáneas aprovisio nadas previamente.
NumberOfInstancesNotFastLaunched	La cantidad de instancias por AMI con el lanzamiento rápido de EC2 habilitado que provocaron un lanzamiento lento debido a la falta de instantáneas aprovisionadas previamen te disponibles en el momento del lanzamiento.
FastLaunchSnapshotUsedToRefillStartTime	La marca de tiempo en la que Amazon EC2 lanzó una nueva imagen desde una AMI con el lanzamiento rápido de EC2 habilitado para crear otra instantánea después de utilizar una instantánea existente.
FastLaunchSnapshotCreationTime	Mide el tiempo que tardó Amazon EC2 en lanzar una instancia y crear una instantánea para una AMI con el lanzamiento rápido de EC2 habilitado.

El rol vinculado a un servicio para el lanzamiento rápido de EC2

Amazon EC2 utiliza roles vinculados a un servicio para los permisos que necesita para llamar a otros Servicios de AWS en su nombre. Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a un Servicio de AWS. Los roles vinculados a servicios ofrecen una manera segura de delegar permisos a Servicios de AWS, ya que solo los servicios vinculados pueden asumir roles vinculados a servicios. Para obtener más información acerca de cómo Amazon EC2 utiliza los roles de IAM, incluidos los roles vinculados a servicios, consulte Roles de IAM para Amazon EC2.

Amazon EC2 utiliza el rol vinculado a un servicio denominado `AWSServiceRoleForEC2FastLaunch` para crear y administrar un conjunto de instantáneas aprovisionadas previamente que reducen el tiempo que lleva iniciar instancias desde la AMI de Windows.

No es necesario crear este rol vinculado a un servicio de forma manual. Cuando comienza a utilizar el lanzamiento rápido de EC2 para la AMI, Amazon EC2 crea automáticamente el rol vinculado a un servicio, si aún no existe.

> **Note**
>
> Si el rol vinculado a un servicio se elimina de la cuenta, puede habilitar el lanzamiento rápido de EC2 para otra AMI de Windows para volver a crear el rol en la cuenta. Si no, puede deshabilitar el lanzamiento rápido de EC2 para la AMI actual y, a continuación, volver a habilitarlo. Sin embargo, al deshabilitar la característica, la AMI utiliza el proceso de inicialización estándar para todas las instancias nuevas, mientras que Amazon EC2 elimina todas las instantáneas aprovisionadas previamente. Después de que se hayan eliminado todas las instantáneas aprovisionadas previamente, puede volver a habilitar el lanzamiento rápido de EC2 para la AMI.

Amazon EC2 no permite editar el rol vinculado a un servicio de `AWSServiceRoleForEC2FastLaunch`. Después de crear un rol vinculado a un servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al mismo. Sin embargo, puede editar la descripción del rol mediante IAM. Para más información, consulte Editar un rol vinculado a un servicio en la Guía del usuario de IAM..

Solo puede eliminar un rol vinculado a un servicio después de eliminar los recursos relacionados. Esto protege los recursos de Amazon EC2 asociados a la AMI de Windows Server de Amazon EC2

con el lanzamiento rápido de EC2 habilitado, ya que no se puede quitar de manera accidental el permiso de acceso a los recursos.

Amazon EC2 es compatible con el rol vinculado a un servicio de lanzamiento rápido de EC2 en todas las regiones en las que el servicio de Amazon EC2 está disponible. Para obtener más información, consulte Regiones.

Permisos concedidos por **`AWSServiceRoleForEC2FastLaunch`**

Amazon EC2 utiliza la política administrada `EC2FastLaunchServiceRolePolicy` para realizar las siguientes acciones:

- `cloudwatch:PutMetricData`: publica datos de métricas asociados con el lanzamiento rápido de EC2 en el espacio de nombres de Amazon EC2.
- `ec2:CreateLaunchTemplate`: crea una platilla de lanzamiento para la AMI de Windows Server de Amazon EC2 con el lanzamiento rápido de EC2 habilitado.
- `ec2:CreateSnapshot`: crea instantáneas aprovisionadas previamente para la AMI de Windows Server de Amazon EC2 con el lanzamiento rápido de EC2 habilitado.
- `ec2:CreateTags`: crea etiquetas para los recursos asociados al lanzamiento y a la aprovisionamiento previo de las instancias de Windows para la AMI de Windows Server de Amazon EC2 con el lanzamiento rápido de EC2 habilitado.
- `ec2:DeleteSnapshots`: elimina todas las instantáneas aprovisionadas previamente asociadas, si el lanzamiento rápido de EC2 está desactivado para una AMI habilitada anteriormente.
- `ec2:DescribeImages`: describir imágenes para todos los recursos.
- `ec2:DescribeInstanceAttribute`: describir atributos de instancias para todos los recursos.
- `ec2:DescribeInstanceStatus`: describir estados de instancias para todos los recursos.
- `ec2:DescribeInstances`: describir instancias para todos los recursos.
- `ec2:DescribeInstanceTypeOfferings`: describir ofertas de tipos de instancias para todos los recursos.
- `ec2:DescribeLaunchTemplates`: describir plantillas de inicialización para todos los recursos.
- `ec2:DescribeLaunchTemplateVersions`: describir versiones de plantillas de inicialización para todos los recursos.
- `ec2:DescribeSnapshots`: describir recursos de instantáneas para todos los recursos.
- `ec2:DescribeSubnets`: describir subredes para todos los recursos.

- `ec2:RunInstances`: lanza las instancias desde una AMI de Windows Server de Amazon EC2 con el lanzamiento rápido de EC2 habilitado para poder realizar los pasos de aprovisionamiento.
- `ec2:StopInstances`: detiene las instancias lanzadas desde una AMI de Windows Server de Amazon EC2 con el lanzamiento rápido de EC2 habilitado para crear instantáneas aprovisionadas previamente.
- `ec2:TerminateInstances`: finaliza una instancia lanzada desde una AMI de Windows Server de Amazon EC2 con el lanzamiento rápido de EC2 habilitado después de crear una instantánea aprovisionada previamente a partir de la instancia.
- `iam:PassRole` permite que el rol vinculado a un servicio `AWSServiceRoleForEC2FastLaunch` lance instancias en su nombre mediante el perfil de instancias de la plantilla de inicialización.

Para obtener más información sobre las políticas administradas por Amazon EC2, consulte Políticas administradas de AWS para Amazon EC2.

Acceso a las claves administradas por el cliente para su uso con AMI cifradas e instantáneas de EBS

Requisito previo

- Para permitir que Amazon EC2 acceda a una AMI cifrada en su nombre, debe contar con un permiso para la acción `createGrant` en la clave administrada por el cliente.

Cuando habilita el lanzamiento rápido de EC2 para una AMI cifrada, Amazon EC2 garantiza que se conceda permiso para el rol `AWSServiceRoleForEC2FastLaunch` para que utilice la clave administrada por el cliente a fin de obtener acceso a la AMI. Este permiso es necesario para iniciar instancias y crear instantáneas aprovisionadas previamente en su nombre.

Uso de los aceleradores de Amazon Elastic Graphics en instancias de Windows

> **Important**
>
> Amazon Elastic Graphics llegó al final de su vida útil el 8 de enero de 2024. Para las cargas de trabajo que requieren aceleración de gráficos, le recomendamos usar instancias G4ad, G4dn o G5 de Amazon EC2.

Amazon Elastic Graphics ofrece una aceleración de gráficos flexible, de bajo costo y de alto rendimiento para sus instancias de Windows. Los aceleradores gráficos elásticos están disponibles en varios tamaños y son una alternativa de bajo costo al uso de tipos de instancia de gráficos GPU (como G3). Cuenta con la flexibilidad de elegir un tipo de instancia que cumpla con las necesidades de computación, memoria y almacenamiento de su aplicación. A continuación, elija el acelerador para su instancia que cumpla con los requisitos gráficos de su carga de trabajo.

Elastic Graphics es adecuado para las aplicaciones que requieren una cantidad pequeña o intermitente de aceleración de gráficos adicional y que usan la compatibilidad de gráficos de OpenGL. Si necesita obtener acceso a GPU completas adjuntas directamente y usar las plataformas de computación en paralelo de DirectX, CUDA u Open Computing Language (OpenCL), use un tipo de instancia de computación acelerada en su lugar.

Contenido

Conceptos básicos de Elastic Graphics

Para usar Elastic Graphics, lance una instancia Windows y especifique un tipo de acelerador para la instancia durante el lanzamiento. AWS busca la capacidad de Elastic Graphics disponible y establece una conexión de red entre su instancia y el acelerador de Elastic Graphics.

> **Note**
>
> No se admiten instancias Bare Metal.

Los aceleradores de Elastic Graphics están disponibles en las siguientes regiones de AWS: `us-east-1`, `us-east-2`, `us-west-2`, `ap-northeast-1`, `ap-southeast-1`, `ap-southeast-2`, `eu-central-1` y `eu-west-1`.

Los siguientes tipos de instancias admiten aceleradores de Elastic Graphics:

- De uso general: M3, M4, M5, M5d, M5dn, M5n, T2, T3

> **Note**
>
> Solo se admiten los tamaños `t2.medium` más grandes y `t3.medium`más grandes.

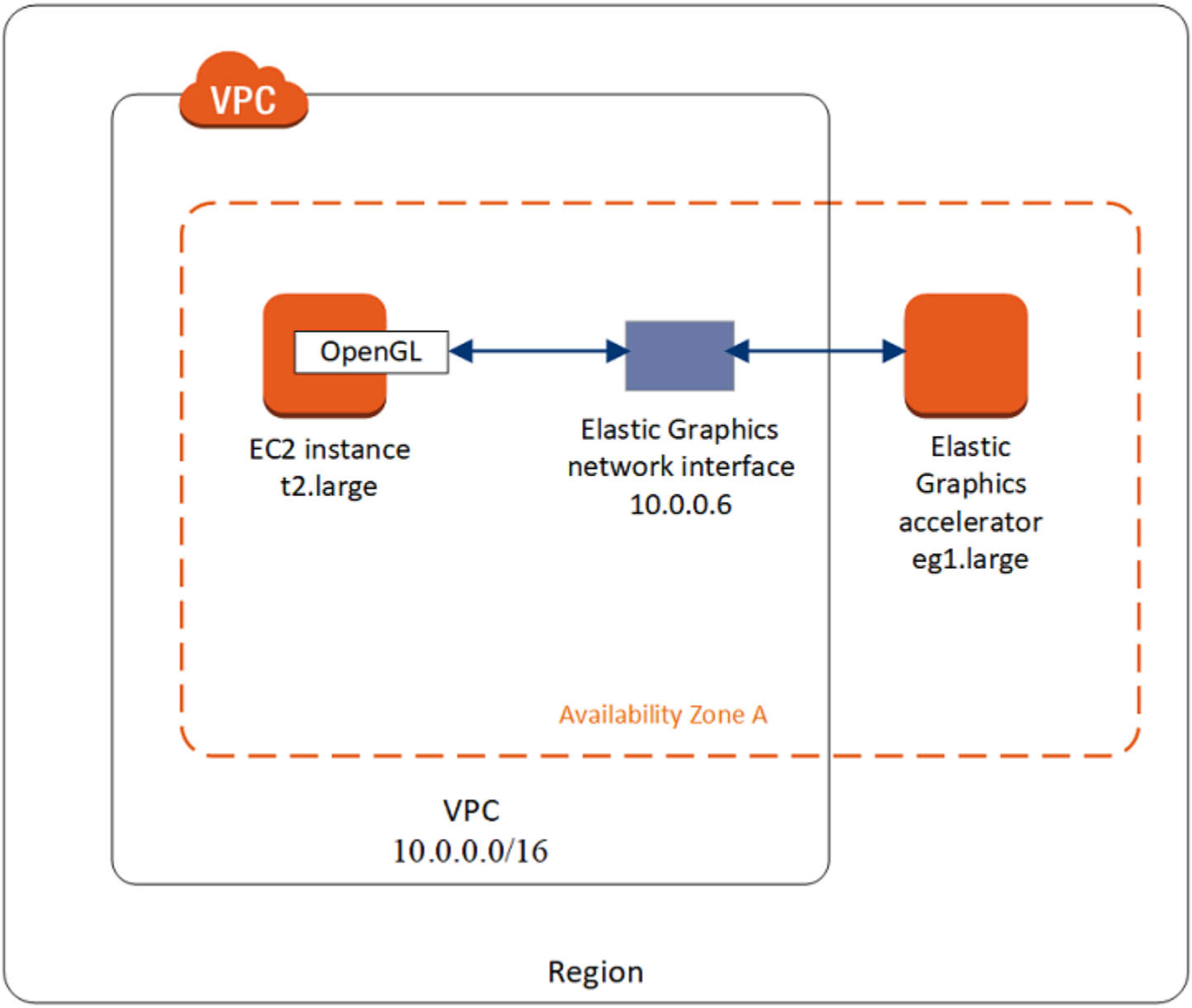
- Optimizadas para computación: C3, C4, C5, C5a, C5ad, C5d, C5n
- Optimizadas para memoria: R3, R4, R5, R5d, R5dn, R5n, X1, X1e, z1d
- Optimizadas para almacenamiento: D2, D3, D3en, H1, I3, I3en
- De computación acelerada: P2, P3, P3dn

Los siguientes aceleradores de Elastic Graphics están disponibles. Puede adjuntar cualquier acelerador de Elastic Graphics a cualquier tipo de instancia admitido.

Acelerador de Elastic Graphics	Memoria gráfica (GB)
`eg1.medium`	1
`eg1.large`	2
`eg1.xlarge`	4
`eg1.2xlarge`	8

Un acelerador de Elastic Graphics no forma parte del hardware de la instancia. En lugar de ello, se conecta a la red a través de una interfaz de red, denominada interfaz de red de Elastic Graphics. Cuando lanza o reinicia una instancia con la aceleración de gráficos, se crea la interfaz de red de Elastic Graphics en la VPC automáticamente.

La interfaz de red de Elastic Graphics se crea en la misma subred y VPC que la instancia y se le asigna una dirección IPv4 privada de esa subred. El acelerador asociado a la instancia Amazon EC2 se asigna desde un grupo de aceleradores disponibles en la misma zona de disponibilidad que su instancia.



Los aceleradores de Elastic Graphics admiten los estándares de la API de OpenGL 4.3 y versiones anteriores, que se pueden usar para las aplicaciones por lotes o la aceleración de gráficos 3D. Una biblioteca de OpenGL optimizada para Amazon incluida en su instancia detecta el acelerador asociado. Dirige las llamadas a la API de OpenGL desde su instancia al acelerador, que procesa las solicitudes y devuelve los resultados. El tráfico entre la instancia y el acelerador usa el mismo ancho de banda que el tráfico de red de la instancia, por lo que recomendamos que disponga del ancho de banda de red adecuado. Póngase en contacto con el proveedor de software si tiene alguna pregunta sobre la compatibilidad y la versión de OpenGL.

De forma predeterminada, el grupo de seguridad predeterminado de su VPC está asociado a la interfaz de red de Elastic Graphics. El tráfico de red de Elastic Graphics usa el protocolo TCP y el puerto 2007. Asegúrese de que el grupo de seguridad de la instancia permite este tráfico. Para obtener más información, consulte Configurar sus grupos de seguridad.

Precios de las Elastic Graphics

Se le cobra cada segundo que un acelerador de Elastic Graphics está asociado a una instancia con el estado `running` cuando el acelerador está en el estado `Ok`. No se le cobrará por un acelerador asociado a una instancia que tenga el estado `pending`, `stopping`, `stopped`, `shutting-down` o `terminated`. Tampoco se le cobra cuando un acelerador tiene el estado `Unknown` o `Impaired`.

Los aceleradores solo están disponible al precio de las instancias bajo demanda. Puede adjuntar un acelerador a una instancia reservada o de spot; sin embargo, se aplica el precio bajo demanda del acelerador.

Para obtener más información, consulte Precios de Amazon Elastic Graphics.

Limitaciones de Elastic Graphics

Antes de empezar a usar aceleradores de Elastic Graphics, tenga en cuenta las siguientes limitaciones:

- Solamente puede asociar aceleradores a instancias de Windows con Microsoft Windows Server 2012 R2 o versiones posteriores. Las instancias Linux no se admiten actualmente.
- Puede asociar un acelerador a una instancia a la vez.
- Sólo puede asociar un acelerador durante el lanzamiento de la instancia. No se puede asociar un acelerador a una instancia existente.
- No puede hibernar una instancia con un acelerador adjunto.
- No puede compartir un acelerador entre instancias.
- No puede desconectar un acelerador de una instancia ni transferirlo a otra instancia. Si ya no necesita un acelerador, debe terminar la instancia. Para cambiar el tipo de acelerador, cree una AMI desde su instancia, termine la instancia y lance una nueva instancia con una especificación de acelerador diferente.
- Las únicas versiones compatibles de la API de OpenGL son la 4.3 y las anteriores. No se admiten DirectX, CUDA ni OpenCL.
- El acelerador de Elastic Graphics no está visible ni accesible desde el administrador de dispositivos de su instancia.

- No puede reservar o programar la capacidad del acelerador.

Trabajar con Elastic Graphics

> **Important**
>
> Amazon Elastic Graphics llegó al final de su vida útil el 8 de enero de 2024. Para las cargas de trabajo que requieren aceleración de gráficos, le recomendamos usar instancias G4ad, G4dn o G5 de Amazon EC2.

Puede lanzar una instancia y asociarla a un acelerador de Elastic Graphics durante el lanzamiento. A continuación, debe instalar manualmente las bibliotecas necesarias en la instancia para permitir la comunicación con el acelerador. Para conocer las limitaciones, consulte Limitaciones de Elastic Graphics.

Tareas

- Configurar sus grupos de seguridad
- Inicie una instancia con un acelerador de Elastic Graphics
- Instalar el software necesario para Elastic Graphics
- Verificar la funcionalidad de Elastic Graphics en su instancia
- Ver información de Elastic Graphics
- Enviar comentarios

Configurar sus grupos de seguridad

Elastic Graphics requiere un grupo auto-referencial de seguridad que permita todo el tráfico entrante y saliente hacia y desde el propio grupo de seguridad. El grupo de seguridad debe incluir las siguientes reglas de entrada y salida:

Entrada

Tipo	Protocolo	Puerto	Origen
Elastic Graphics	TCP	2007	El ID del grupo de seguridad (su propio ID de recurso)

Salida

Tipo	Protocolo	Intervalo de puertos	Destino
Elastic Graphics	TCP	2007	El ID del grupo de seguridad (su propio ID de recurso)

Si utiliza la consola de Amazon EC2 para lanzar su instancia con un acelerador de Elastic Graphics, puede permitir que el asistente de lanzamiento de instancias cree automáticamente reglas de grupo de seguridad requeridas o puede seleccionar una seguridad que ha creado anteriormente.

Si está iniciando su instancia utilizando el comando AWS CLI o un SDK, debe especificar un grupo de seguridad que creó anteriormente.

Para crear un grupo de seguridad para Elastic Graphics

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Grupos de seguridad y, a continuación, elija Crear grupo de seguridad.
3. En la ventana Crear grupo de seguridad, haga lo siguiente:
    a. En Nombre del grupo de seguridad, ingrese un nombre descriptivo para el grupo de seguridad, como, por ejemplo, `Elastic Graphics security group`.
    b. (Opcional) En Descripción, ingrese una breve descripción del grupo de seguridad.
    c. EnVPC, seleccione la VPC en la que desea utilizar Elastic Graphics.
    d. Elija Crear grupo de seguridad.
4. En el panel de navegación, seleccione Grupos de seguridad, seleccione el grupo de seguridad de que acaba de crear y, en la pestaña Detalles, copie el ID de grupo de seguridad.
5. En la pestaña Inbound (Entrada), elija Edit inbound rules (Editar reglas de entrada) y, a continuación, agregue lo siguiente:
    a. Seleccione Agregar regla.
    b. En Type (Tipo), elija Elastic Graphics.
    c. En Source type (Tipo de origen), elija Custom (Personalizado).
    d. En Fuente, pegue el ID del grupo de seguridad que copió anteriormente.

e. Seleccione Guardar reglas.

6. En la pestaña Outbound rules (Reglas salientes) seleccione Edit outbound rules (Editar reglas salientes) y luego realice lo siguiente:

   a. Seleccione Agregar regla.

   b. En Type (Tipo), elija Elastic Graphics.

   c. Para Tipos de destino, elija Custom (Personalizado).

   d. Para Destino, pegue el ID del grupo de seguridad que copió anteriormente.

   e. Seleccione Guardar reglas.

Para obtener más información, consulte Grupos de seguridad de Amazon EC2 para instancias EC2.

Inicie una instancia con un acelerador de Elastic Graphics

Puede asociar un acelerador de Elastic Graphics a una instancia durante el lanzamiento. A continuación se enumeran las posibles razones por las que se puede producir un error en el lanzamiento:

- Capacidad insuficiente del acelerador de Elastic Graphics.
- Se ha superado el límite de aceleradores de Elastic Graphics en la región.
- No hay suficientes direcciones IPv4 privadas en su VPC para crear una interfaz de red para el acelerador.

Para obtener más información, consulte Limitaciones de Elastic Graphics.

Para asociar un acelerador Elastic Graphics durante el lanzamiento de instancia (consola)

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel, elija Iniciar instancia.
3. En Nombre y etiquetas, ingrese un valor en Nombre. Si lo desea, puede elegir Agregar etiquetas adicionales para agregar más etiquetas a los recursos asociados a la instancia que se lanzará.
4. En Imágenes de aplicaciones y sistema operativo (Imagen de máquina de Amazon), seleccione una AMI de Windows.
5. En Tipo de instancia, elija un tipo de instancia admitido. Para obtener más información, consulte Conceptos básicos de Elastic Graphics.

6. (Opcional) En Par de claves (inicio), para Nombre de par de claves seleccione un par de claves existente o cree uno nuevo.
7. Junto a Configuración de red, seleccione Editar y, a continuación, especifique la configuración de red que se utilizará en la instancia.
   a. En Red, seleccione una VPC para la instancia.
   b. En Subred, seleccione la subred en la que desea iniciar la instancia.
   c. En Firewall (grupos de seguridad) puede utilizar el grupo de seguridad que creó de manera manual en Configurar sus grupos de seguridad o dejar que la consola cree un grupo de seguridad con las reglas de entrada y salida necesarias. Añada grupos de seguridad adicionales según sea necesario.
8. (Opcional) En Configurar almacenamiento, configure el tamaño del volumen raíz y agregue volúmenes adicionales según sea necesario.
9. Amplíe la sección Detalles avanzados.
10. En Detalles avanzados, en GPU elástica, seleccione un tipo de acelerador de Elastic Graphics.
11. En el panel Resumen, elija Iniciar instancia.

Para asociar un acelerador Elastic Graphics durante el lanzamiento de instancia (AWS CLI)

Puede utilizar el comando de la AWS CLI run-instances con el siguiente parámetro:

```
--elastic-gpu-specification Type=eg1.medium
```

Para el parámetro `--security-group-ids`, debe incluir un grupo de seguridad que disponga de las reglas de entrada y salida necesarias. Para obtener más información, consulte Configurar sus grupos de seguridad.

Para asociar un acelerador de Elastic Graphics durante el lanzamiento de instancia (Tools for Windows PowerShell)

Utilice el comando New-EC2Instance Herramientas para Windows PowerShell.

Instalar el software necesario para Elastic Graphics

Si lanzó su instancia con una AMI de Windows de AWS actual, el software necesario se instala automáticamente durante el primer arranque. Si lanzó su instancia con las AMI de Windows que no

instalan automáticamente el software necesario, debe instalar manualmente el software necesario en la instancia.

Para instalar el software necesario para Elastic Graphics (si es necesario)

1. Conéctese a la instancia.
2. Descargue el instalador de Elastic Graphics y ábralo. El administrador de instalación se conecta al punto de conexión de Elastic Graphics y descarga la última versión del software necesario.

   > **Note**
   >
   > Si el enlace de descarga no funciona, pruebe con otro navegador o copie la dirección del enlace y péguela en una nueva pestaña del navegador.

3. Reinicie la instancia para verificar que funciona.

Verificar la funcionalidad de Elastic Graphics en su instancia

Los paquetes de Elastic Graphics de su instancia incluyen herramientas que puede usar para ver el estado del acelerador y para verificar que los comandos de OpenGL desde su instancia al acelerador funcionan.

Si la instancia se lanzó con una AMI que no tenía los paquetes de Elastic Graphics preinstalados, puede descargarlos e instalarlos usted mismo. Para obtener más información, consulte Instalar el software necesario para Elastic Graphics.

Puede utilizar uno de los métodos siguientes para verificar la funcionalidad de Elastic Graphics en la instancia.

> **Note**
>
> Si el monitor de estado de Elastic Graphics o la herramienta de la línea de comandos devuelve un resultado inesperado, consulte Resolver problemas de estado incorrecto.

Elastic Graphics status monitor

Puede usar la herramienta de monitor de estado para ver información sobre el estado de un acelerador de Elastic Graphics. De forma predeterminada, esta herramienta está disponible en el

área de notificaciones de la barra de herramientas de su instancia Windows y muestra el estado del acelerador de gráficos. A continuación se muestran los posibles valores.

Buen estado

El acelerador de Elastic Graphics está habilitado y tiene el estado correcto.

Updating

El estado del acelerador de Elastic Graphics se está actualizando actualmente. Puede que se tarde unos minutos en mostrar el estado.

Fuera de servicio

El acelerador de Elastic Graphics está fuera de servicio. Para obtener más información acerca del error, elija Read More (Leer más).

Elastic Graphics command line tool

Puede utilizar la herramienta de línea de comandos de Elastic Graphics, `egcli.exe`, para comprobar el estado del acelerador. Si existe un problema con el acelerador, la herramienta devuelve un mensaje de error.

Para lanzar la herramienta, abra un símbolo del sistema desde dentro de la instancia y ejecute el siguiente comando:

```
C:\Program Files\Amazon\EC2ElasticGPUs\manager\egcli.exe
```

La herramienta también es compatible con los siguientes parámetros:

`--json`, `-j`

Indica si mostrar el mensaje JSON. Los valores posibles son `true` y `false`. El valor predeterminado es `true`.

`--imds`, `-i`

Indica si comprobar los metadatos de la instancia para la disponibilidad del acelerador. Los valores posibles son `true` y `false`. El valor predeterminado es `true`.

A continuación, se muestra un ejemplo del resultado. Un estado de `OK` indica que el acelerador está habilitado y está en buen estado.

```
EG Infrastructure is available.
Instance ID egpu-f6d94dfa66df4883b284e96db7397ee6
Instance Type eg1.large
EG Version 1.0.0.885 (Manager) / 1.0.0.95 (OpenGL Library) / 1.0.0.69 (OpenGL
 Redirector)
EG Status: Healthy
JSON Message:
{
  "version": "2016-11-30",
  "status": "OK"
}
```

Los siguientes son valores posibles para `status`:

`OK`

El acelerador de Elastic Graphics está habilitado y tiene el estado correcto.

`UPDATING`

El controlador de Elastic Graphics se está actualizando.

`NEEDS_REBOOT`

El controlador de Elastic Graphics se ha actualizado y es necesario reiniciar la instancia Amazon EC2.

`LOADING_DRIVER`

El controlador de Elastic Graphics se está cargando.

`CONNECTING_EGPU`

El controlador de Elastic Graphics está comprobando la conectividad con el acelerador de Elastic Graphics.

`ERROR_UPDATE_RETRY`

Se produjo un error al actualizar el controlador de Elastic Graphics. Se recuperará una actualización pronto.

`ERROR_UPDATE`

Se produjo un error irrecuperable al actualizar el controlador de Elastic Graphics.

`ERROR_LOAD_DRIVER`

Se ha producido un error en la carga del controlador de Elastic Graphics.

`ERROR_EGPU_CONNECTIVITY`

No se ha podido obtener acceso al acelerador de Elastic Graphics.

Ver información de Elastic Graphics

Puede ver la información sobre el acelerador de Elastic Graphics asociado a su instancia.

Para ver información sobre un acelerador de Elastic Graphics (consola)

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instances (Instancias) y seleccione la instancia.
3. En la pestaña Detalles, busque el ID de gráficos elásticos. Elija el ID para ver la siguiente información sobre el acelerador de Elastic Graphics:
   - Estado de la conexión
   - Tipo
   - Estado

Para ver información sobre un acelerador de Elastic Graphics (AWS CLI)

Puede utilizar el comando describe-elastic-gpus de la AWS CLI:

```
aws ec2 describe-elastic-gpus
```

Puede utilizar el comando describe-network-interfaces de la AWS CLI y filtrar por ID de propietario para ver información sobre la interfaz de red de Elastic Graphics.

```
aws ec2 describe-network-interfaces --filters "Name=attachment.instance-owner-
id,Values=amazon-elasticgpus"
```

Para ver información sobre un acelerador de Elastic Graphics (Tools for Windows PowerShell)

Use los siguientes comandos:

- Get-EC2ElasticGpu

- Get-EC2NetworkInterface

Para ver información acerca de un acelerador de Elastic Graphics mediante los metadatos de la instancia

1. Conecte su instancia Windows que utiliza un acelerador de Elastic Graphics.
2. Aplique alguna de las siguientes acciones:
   - Desde PowerShell, utilice el siguiente cmdlet:

     ```
     PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/elastic-gpus/associations/egpu-f6d94dfa66df4883b284e96db7397ee6
     ```

   - Desde el explorador web, pegue la siguiente URL en el campo de dirección:

     ```
     http://169.254.169.254/latest/meta-data/elastic-gpus/associations/egpu-f6d94dfa66df4883b284e96db7397ee6
     ```

Enviar comentarios

Puede enviar comentarios sobre su experiencia con Elastic Graphics para que el equipo puede mejorarlas.

Para enviar comentarios mediante el monitor de estado de Elastic Graphics

1. En la zona de notificación de la barra de tareas en su instancia Windows, abra el monitor de estado de Elastic Graphics.
2. En la esquina inferior izquierda, elija Feedback (Comentarios).
3. Introduzca sus comentarios y elija Submit (Enviar).

Mantenimiento de Elastic Graphics

> **Important**
>
> Amazon Elastic Graphics llegó al final de su vida útil el 8 de enero de 2024. Para las cargas de trabajo que requieren aceleración de gráficos, le recomendamos usar instancias G4ad, G4dn o G5 de Amazon EC2.

AWS puede determinar que el estado de un acelerador de Elastic Graphics es incorrecto si:

- Es necesaria una actualización de seguridad o infraestructura
- Es necesaria una actualización de software
- Existe algún problema con el host subyacente

Cuando AWS determina que el estado de un acelerador de Elastic Graphics es incorrecto, programa la retirada del acelerador. AWS le notifica que está pendiente la retirada del acelerador, y le proporciona los pasos correctivos que debe seguir.

Temas

¿Cómo se me notificará?

Cuando AWS programa la retirada de un acelerador de Elastic Graphics, envía una notificación sobre la retirada del acelerador a AWS Health Dashboard. Asimismo, AWS envía un email a la dirección de email asociada a la cuenta de AWS. Se trata de la misma dirección de email que se utiliza para iniciar sesión en la AWS Management Console.

> **Note**
>
> Si utiliza una cuenta de email que no revisa periódicamente, emplee AWS Health Dashboard para determinar si está programada la retirada de alguno de los aceleradores de Elastic Graphics. También puede cambiar la información de contacto de la cuenta de AWS en la página Account Settings (Configuración de la cuenta).

En la notificación sobre la retirada se proporciona lo siguiente:

- El ID de la instancia a la que está adjuntado el acelerador
- Información sobre el problema que afecta al acelerador
- La fecha de retirada del acelerador
- Los pasos correctivos que debe seguir

¿Qué tengo que hacer?

Cuando se le notifique que se ha programado la retirada de un acelerador de Elastic Graphics, debe detener e iniciar la instancia a la que esté adjuntado el acelerador, para que el acelerador antiguo e incorrecto se pueda sustituir por uno nuevo y correcto.

Se recomienda cerrar las aplicaciones gráficas que se estén ejecutando en la instancia antes de detener y reiniciar la instancia.

> **Important**
>
> Si no detiene e inicia la instancia antes de la fecha de retirada programada, se detendrá automáticamente el acelerador asociado a la instancia, lo que podría provocar que las aplicaciones dejen de funcionar.
> Debe detener e iniciar la instancia. Al reiniciar la instancia, el acelerador incorrecto no se sustituirá por uno correcto.

¿Qué ocurre cuando un acelerador llega a su fecha de retirada?

Cuando un acelerador de Elastic Graphics incorrecto llega a su fecha de retirada programada, AWS lo termina de manera permanente. Para recibir un reemplazo para un acelerador incorrecto, ya sea antes o después de la fecha de retirada, debe detener e iniciar la instancia a la que esté adjuntado el acelerador.

Si no detiene e inicia la instancia antes de la fecha de retirada programada, se detendrá automáticamente el acelerador asociado a la instancia, lo que podría provocar que las aplicaciones dejen de funcionar.

Utilice las CloudWatch métricas que se van a supervisar Elastic Graphics

> **Important**
>
> Amazon Elastic Graphics llegó al final de su vida útil el 8 de enero de 2024. Para las cargas de trabajo que requieren aceleración de gráficos, le recomendamos usar instancias G4ad, G4dn o G5 de Amazon EC2.

Puede monitorizar su acelerador de Elastic Graphics mediante Amazon CloudWatch, que recopila métricas sobre el rendimiento de su acelerador. Estas estadísticas se registran durante un periodo

de dos semanas, de forma que pueda tener acceso a información histórica y obtener una mejor perspectiva sobre el rendimiento de su servicio.

De forma predeterminada, los aceleradores de Elastic Graphics envían datos métricos a CloudWatch en periodos de 5 minutos.

Para obtener más información sobre Amazon CloudWatch, consulte la Guía del usuario de Amazon CloudWatch.

Métricas de Elastic Graphics

El espacio de nombres de `AWS/ElasticGPUs` incluye las siguientes métricas para Elastic Graphics.

Métrica	Descripción
GPUConnectivityCheckFailed	Indica si la conectividad al acelerador Elastic Graphics está activa o ha producido un error. Un valor de cero (0) indica que la conexión está activa. Un valor de uno (1) indica un error de conexión. Unidades: recuento
GPUHealthCheckFailed	Indica si el acelerador de Elastic Graphics ha superado una comprobación de estado en el último minuto. Un valor de cero (0) indica que se ha superado la comprobación de estado. Un valor de uno (1) indica que no se ha superado una comprobación de estado. Unidades: recuento
GPUMemoryUtilization	La memoria de la GPU utilizada. Unidades: MiB

Dimensiones de Elastic Graphics

Puede filtrar los datos de métricas para sus aceleradores de Elastic Graphics mediante las siguientes dimensiones.

Dimensión	Descripción
`EGPUId`	Filtra los datos por el acelerador de Elastic Graphics.
`InstanceId`	Filtra los datos por la instancia a la que se asocia el acelerador de Elastic Graphics.

Ver métricas de CloudWatch para Elastic Graphics

Las métricas se agrupan en primer lugar por el espacio de nombres de servicio y, a continuación, por las dimensiones compatibles. Puede seguir los siguientes procedimientos para ver las métricas de sus aceleradores de Elastic Graphics.

Para consultar las métricas de Elastic Graphics mediante la consola de CloudWatch

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. Si es necesario, cambie la región. En la barra de navegación, seleccione la región donde reside su acelerador de Elastic Graphics. Para obtener más información, consulte Regiones y puntos de enlace.
3. En el panel de navegación, seleccione Metrics (Métricas).
4. En All metrics (Todas las métricas), seleccione Elastic Graphics y Elastic Graphics Metrics (Métricas de Elastic Graphics).

Para ver las métricas de Elastic Graphics (AWS CLI)

Utilice el siguiente comando list-metrics:

```
aws cloudwatch list-metrics --namespace "AWS/ElasticGPUs"
```

Crear alarmas de CloudWatch para supervisar Elastic Graphics

Puede crear una alarma de CloudWatch que envíe un mensaje de Amazon SNS cuando la alarma cambie de estado. Una alarma vigila una única métrica durante el período especificado y envía una notificación a un tema de Amazon SNS según el valor de la métrica relativo a un determinado umbral durante varios períodos de tiempo.

Por ejemplo, puede crear una alarma que monitorice el estado de un acelerador de Elastic Graphics y envíe una notificación cuando el acelerador de gráficos no supere una comprobación de estado durante tres periodos consecutivos de cinco minutos.

Para crear una alarma para un estado del acelerador de Elastic Graphics

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, elija Alarms, Create Alarm.
3. Elija Select metric (Seleccionar métrica), Elastic Graphics y Elastic Graphics Metrics (Métricas de Elastic Graphics).
4. Seleccione la métrica GPUHealthCheckFailed y elija Select metric (Seleccionar métrica).
5. Configure la alarma del modo siguiente:
   a. En Alarm details (Detalles de alarma), escriba un nombre y una descripción de la alarma. En Whenever (Siempre que), elija >= y escriba 1.
   b. En Actions (Acciones), seleccione una notificación existente o elija New list (Nueva lista).
   c. Elija Create Alarm.

Solución de problemas

> **Important**
>
> Amazon Elastic Graphics llegó al final de su vida útil el 8 de enero de 2024. Para las cargas de trabajo que requieren aceleración de gráficos, le recomendamos usar instancias G4ad, G4dn o G5 de Amazon EC2.

A continuación se muestran los errores habituales y los pasos para solucionarlos.

Contenido

- Detenga e inicie la instancia.
- Verifique los componentes instalados
- Consultar los registros de Elastic Graphics

- ¿Por qué veo varias ENI?

Investigación de problemas de rendimiento de las aplicaciones

Elastic Graphics utiliza la red de la instancia para enviar comandos de OpenGL a una tarjeta gráfica conectada de forma remota. Además, se suele utilizar una tecnología de acceso remoto para obtener acceso al escritorio que ejecuta una aplicación de OpenGL con un acelerador de Elastic Graphics. Es importante distinguir entre un problema de rendimiento relacionado con la presentación de OpenGL o con la tecnología de acceso remoto del escritorio.

Problemas de rendimiento de la presentación de OpenGL

El rendimiento de presentación de OpenGL se determina por el número de comandos y fotogramas de OpenGL generados en la instancia remota.

El rendimiento de presentación pueden variar en función de los siguientes factores:

- Rendimiento del acelerador de Elastic Graphics
- Rendimiento de la red
- Rendimiento de la CPU
- Modelo de presentación o complejidad del escenario
- Funcionamiento de la aplicación de OpenGL

Una forma sencilla de evaluar el rendimiento consiste en presentar el número de fotogramas mostrados en la instancia remota. Los aceleradores de Elastic Graphics muestran un máximo de 25 FPS en la instancia remota a fin de alcanzar la mejor calidad percibida a la vez que se reduce el uso de la red.

Para mostrar el número de fotogramas producidos

1. Abra el siguiente archivo en un editor de texto. Si el archivo no existe, créelo.

```
C:\Program Files\Amazon\EC2ElasticGPUs\conf\eg.conf
```

2. Identifique la sección `[Application]` o añádala si no está presente, y añada el siguiente parámetro de configuración:

```
[Application]
show_fps=1
```

3. Reinicie la aplicación y compruebe de nuevo el número de FPS.

Si FPS alcanza los 15-25 FPS al actualizar la escena representada, el acelerador de Elastic Graphics está funcionando al máximo. Probablemente, los demás problemas de rendimiento experimentados estén relacionados con el acceso remoto al escritorio de la instancia. En tal caso, consulte la sección Problemas de rendimiento del acceso remoto.

Si el número de FPS es inferior a 15, pruebe lo siguiente:

- Mejore el rendimiento del acelerador de Elastic Graphics seleccionando un tipo de acelerador de gráficos más potente.
- Mejore el rendimiento general de la red siguiendo estas recomendaciones:
  - Compruebe la cantidad de ancho de banda entrante y saliente a y desde el punto de conexión del acelerador de Elastic Graphics. El punto de conexión del acelerador de Elastic Graphics se puede recuperar con el siguiente comando de PowerShell:

```
PS C:\> (Invoke-WebRequest http://169.254.169.254/latest/meta-data/elastic-gpus/
associations/[ELASTICGPU_ID]).content
```

  - El tráfico de red desde la instancia al punto de conexión del acelerador de Elastic Graphics está relacionado con el volumen de comandos que produce la aplicación de OpenGL.
  - El tráfico de red desde el punto de conexión del acelerador de Elastic Graphics a la instancia está relacionado con el número de fotogramas generados por el acelerador de gráficos.
  - Si ve que el uso de la red se acerca a la velocidad de red máxima de las instancias, pruebe a usar una instancia con una velocidad de red mayor.
- Mejore el rendimiento de la CPU:
  - Las aplicaciones puede requerir muchos recursos de CPU además de los que requiere el acelerador de Elastic Graphics. Si el Administrador de tareas de Windows indica un uso elevado de recursos de CPU, pruebe a usar una instancia con una potencia de CPU mayor.

Problemas de rendimiento del acceso remoto

A una instancia con un acelerador de Elastic Graphics asociado se puede tener acceso mediante diferentes tecnologías de acceso remoto. El rendimiento y la calidad pueden variar en función de los siguientes factores:

- La tecnología de acceso remoto
- El rendimiento de las instancias
- El rendimiento del cliente
- La latencia y el ancho de banda de red entre el cliente y la instancia

Las opciones posibles para el protocolo de acceso remoto son las siguientes:

- Conexión a Escritorio remoto de Microsoft
- NICE DCV
- VNC

Para obtener más información sobre la optimización, consulte el protocolo específico.

Resolver problemas de estado incorrecto

Si el acelerador de Elastic Graphics tiene un estado incorrecto, utilice los siguientes pasos de solución de problemas para resolver el problema.

Verifique la configuración de las instancias

Si la herramienta de la línea de comandos de Elastic Graphics (`egcli.exe`) devuelve un resultado similar al siguiente, asegúrese de que el grupo de seguridad esté configurado correctamente y que se haya lanzado la instancia con Instance Metadata Service habilitado.

```
EG Version 1.0.7.4240 (Manager) / N/A (OpenGL Library) / N/A (OpenGL Redirector)
EG Status: Out Of Service
Something prevented the EG Infrastructure to work properly.
```

Detenga e inicie la instancia.

Si el acelerador de Elastic Graphics tiene un estado incorrecto, detener la instancia e iniciarla de nuevo es la opción más sencilla. Para obtener más información, consulte Detención e inicio de sus instancias de forma manual.

> **Warning**
>
> Cuando detiene una instancia, se borran los datos contenidos en todos los volúmenes de almacén de instancias. Para conservar los datos de los volúmenes del almacén de instancias, asegúrese de realizar una copia de seguridad de ellos en un almacenamiento persistente.

Verifique los componentes instalados

Abra el Panel de control de Windows y confirme que los siguientes componentes están instalados:

- Amazon Elastic Graphics Manager
- Amazon Elastic Graphics OpenGL Library
- Amazon EC2 Elastic GPUs OpenGL Redirector

Si falta alguno de estos elementos, debe instalarlos manualmente. Para obtener más información, consulte Instalar el software necesario para Elastic Graphics.

Consultar los registros de Elastic Graphics

Abra el Visor de eventos de Windows, expanda la sección Registros de aplicaciones y servicios y busque los errores en los siguientes registros de eventos:

- EC2ElasticGPUs
- GUI de EC2ElasticGPUs

¿Por qué veo varias ENI?

Al llamar a StartInstances en una instancia de EC2 con un acelerador Elastic Graphics, se crea una nueva interfaz de red elástica (ENI) en la instancia para permitir el envío de comandos OpenGL a la tarjeta gráfica conectada de forma remota.

Si llama a StartInstances muchas veces en un periodo corto (unos segundos o menos) en la misma instancia de EC2, se crea una nueva interfaz de red en cada llamada. Sin embargo:

- El acelerador de Elastic Graphics solo utilizará una interfaz de red.

- Las interfaces de red adicionales no incurren en ningún cargo y se liberarán automáticamente en 24 horas.

Instalar WSL en su instancia de Windows

Puede descargar Windows Subsystem for Linux (WSL) de forma gratuita en su instancia de Windows Subsystem for Linux (WSL). Al instalar WSL, puede ejecutar herramientas de línea de comandos nativas de Linux directamente en su instancia de Windows y usar las herramientas de Linux para crear scripts, junto con su escritorio de Windows tradicional. Puede cambiar fácilmente entre Linux y Windows en una sola instancia de Windows, lo que puede resultarle útil en un entorno de desarrollo.

Para obtener más información sobre WSL, consulte la documentación de Windows Subsystem for Linux en el sitio web de Microsoft Build.

Limitaciones

- WSL está disponible en dos versiones: WSL 1 y WSL 2.
  - Para las instancias de EC2 `.metal`, puede instalar WSL 1 o WSL 2.
  - En el caso de las instancias de EC2 virtualizadas, debe instalar WSL 1.
- Para los sistemas operativos Windows Server, WSL solo se puede instalar en instancias que ejecuten lo siguiente:
  - Windows Server 2019
  - Windows Server 2022

Instalar WSL

Las siguientes instrucciones instalan WSL en una instancia de EC2 que se ejecuta en Windows Server 2022. Para obtener instrucciones para instalar WSL en una instancia de EC2 que ejecute Windows Server 2019, consulte Instalación de WSL en versiones anteriores de Windows Server en el sitio web de Microsoft. Después de seguir esas instrucciones, puede utilizar el paso 3 de las instrucciones siguientes para configurar WSL a fin de utilizar WSL 1.

Instalación de WSL 1

1. Para instalar WSL, ejecute el siguiente comando de instalación estándar en su instancia de EC2, pero asegúrese de habilitar WSL 1 al incluir `--enable-wsl1`. Por defecto, se instala WSL 2.

Si la instancia se lanzó con un tipo de instancia virtualizado, debe completar el paso 3 de este procedimiento para establecer la versión en WSL 1.

```
wsl --install --enable-wsl1 --no-launch
```

2. Reinicie la instancia de EC2.

```
shutdown -r -t 20
```

3. Para configurar WSL para utilizar WSL 1, ejecute el siguiente comando en su instancia. Para obtener más información sobre cómo configurar la versión de WSL, consulte los pasos de instalación manual para versiones anteriores de WSL en el sitio web de Microsoft Build.

```
wsl --set-default-version 1
```

4. Instale la distribución predeterminada.

```
wsl --install
```

Instalación de WSL 2

- Para instalar WSL, ejecute el siguiente comando de instalación estándar en su instancia de EC2. Por defecto, se instala WSL 2. Si está instalando WSL en una instancia `.metal`, este es el único paso que debe realizar.

```
wsl --install
```

Para obtener más información, consulte Instalar Linux en Windows con WSL en el sitio web de Microsoft Build.

Actualizar una instancia de Windows Amazon EC2 a una versión más reciente de Windows Server

Existen dos métodos para actualizar una versión anterior de Windows Server cuando se ejecuta en una instancia: actualización local y migración (también denominada actualización en paralelo). Con la actualización local, se actualizan los archivos del sistema operativo, pero la configuración y los archivos personales permanecen intactos. La migración implica capturar los ajustes, las

configuraciones y los datos y llevarlos a un sistema operativo más reciente en una instancia Amazon EC2 nueva.

Tradicionalmente, Microsoft ha recomendado migrar a una versión más nueva de Windows Server en lugar de actualizarla. Al migrar se pueden registrar menos errores o problemas de actualización, pero puede tardar más tiempo que una actualización in situ, debido a la necesidad de aprovisionar una nueva instancia, planificar y trasladar aplicaciones y ajustar los valores de configuración de la nueva instancia. Una actualización in situ puede ser más rápida, pero las incompatibilidades de software pueden producir errores.

Contenido

Cómo realizar una actualización local en su instancia de Windows

Antes de realizar una actualización local, debe determinar qué controladores de red está ejecutando la instancia. Con los controladores de red PV, puede obtener acceso a la instancia con el Escritorio remoto. Las instancias usan controladores de AWS PV, Intel Network Adapter o Enhanced Networking. Para obtener más información, consulte Controladores paravirtuales para instancias de Windows.

Antes de iniciar una actualización in situ

Realice las siguientes tareas y anote los siguientes datos importantes antes de empezar la actualización local.

- Lea la documentación de Microsoft para comprender los requisitos de actualización, los problemas conocidos y las restricciones. Consulte también las instrucciones oficiales para aplicar actualizaciones.
  - Opciones de actualización de Windows Server 2012
  - Opciones de actualización de Windows Server 2012 R2

  - Opciones de actualización y conversión de Windows Server 2016
  - Opciones de actualización y conversión de Windows Server 2019
  - Opciones de actualización y conversión de Windows Server 2022
  - Centro de actualización de Windows Server
- Recomendamos realizar una actualización del sistema operativo en instancias con al menos dos vCPU y 4 GB de RAM. Si lo necesita, puede cambiar la instancia a un mayor tamaño del mismo tipo (t2.small a t2.large, por ejemplo), realizar la actualización y, a continuación, volver a cambiar al tamaño original. Si tiene que mantener el tamaño de la instancia, puede monitorear el progreso utilizando la Captura de pantalla de consola de instancia. Para obtener más información, consulte Cambie el tipo de instancia.
- Verifique que el volumen raíz en su instancia de Windows tiene espacio de disco suficiente. El proceso de Windows Setup podría no advertirle de que el espacio de disco es insuficiente. Para obtener información acerca de cuánto espacio de disco se necesita para actualizar un sistema operativo concreto, consulte la documentación de Microsoft. Si el volumen no dispone de suficiente espacio, se puede ampliar. Para obtener más información, consulte Volúmenes elásticos de Amazon EBS en la Guía del usuario de Amazon EBS.
- Determine la ruta de actualización. Debe actualizar el sistema operativo a la misma arquitectura. Por ejemplo, debe actualizar un sistema de 32 bits a un sistema de 32 bits. Windows Server 2008 R2 y las versiones posteriores son solo de 64 bits.
- Deshabilite el software antivirus y antispyware y los firewalls. Estos tipos de software pueden entrar en conflicto con el proceso de actualización. Vuelva a habilitar el software antivirus y antispyware y los firewalls una vez que finalice la actualización.
- Actualice a los controladores más recientes, tal como se describe en Migración de una instancia de Windows a un tipo de instancia de generación actual.
- Upgrade Helper Service solo admite instancias que ejecuten controladores Citrix PV. Si la instancia ejecuta controladores Red Hat, primero debe actualizar esos controladores manualmente.

Actualización in situ de una instancia con controladores AWS PV, Intel Network Adapter o Enhanced Networking

Siga este procedimiento para actualizar una instancia de Windows Server con los controladores de red AWS PV, Intel Network Adapter o Enhanced Networking.

Para ejecutar la actualización local

1. Cree una AMI del sistema que tenga pensado actualizar con fines de copia de seguridad o de prueba. A continuación, puede realizar la actualización en la copia para simular un entorno de prueba. Si la actualización se completa, puede cambiar el tráfico a esta instancia con un bajo tiempo de inactividad. Si la actualización da error, puede volver a la copia de seguridad. Para obtener más información, consulte Creación de una AMI basada en Amazon EBS.
2. Asegúrese de que la instancia con Windows Server use los controladores de red más recientes.
   a. Para actualizar el controlador de PV de AWS, consulteActualizar controladores PV en instancias de Windows.
   b. Para actualizar el controlador de ENA, consulte Instalación del controlador Elastic Network Adapter (ENA).
   c. Para actualizar los controladores de Intel, consulte Habilitación de redes mejoradas con la interfaz de Intel 82599 VF en instancias EC2.
3. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
4. En el panel de navegación, seleccione Instances (Instancias). Localice la instancia. Anote el ID de instancia y la zona de disponibilidad de la instancia. Necesita esta información más tarde en este mismo procedimiento.
5. Si va a actualizar Windows Server 2012 o 2012 R2 a Windows Server 2016, 2019 o 2022, antes de continuar, realice las siguientes acciones en la instancia:
   a. Desinstale el servicio EC2Config. Para obtener más información, consulte Detener, reiniciar, eliminar o desinstalar EC2Config.
   b. Instale EC2Launch v1 o el agente de EC2Launch v2. Para obtener más información, consulte Configurar una instancia de Windows utilizando EC2Launch y Configurar una instancia de Windows mediante EC2Launch v2.
   c. Instalar el SSM Agent de AWS Systems Manager. Para obtener más información, consulte Usar el SSM Agent en la Guía del usuario de AWS Systems Manager.
6. Cree un volumen a partir de una instantánea de un medio de instalación de Windows Server.
   a. En el panel de navegación, bajo Elastic Block Store, elija “Snapshots” (Instantáneas).
   b. En la barra del filtro, elija Instantáneas públicas.
   c. En la barra de búsqueda, especifique los siguientes filtros:
      - Seleccione Alias del propietario, = y amazon.

- Seleccione Descripción y comience a escribir **`Windows`**. Seleccione el filtro de Windows que coincida con la arquitectura del sistema y la preferencia de idioma de la actualización. Por ejemplo, seleccione Windows 2019 English Installation Media si la actualización corresponde a Windows Server 2019.

d. Seleccione la casilla de verificación situada junto a la instantánea que corresponda a la arquitectura del sistema y la preferencia de idioma a la que vaya a realizar la actualización y, a continuación, elija Acciones, Crear volumen a partir de una instantánea.

e. En la página Crear volumen, elija la zona de disponibilidad que corresponda a la instancia de Windows y seleccione Crear volumen.

7. En el encabezado Volumen creado correctamente vol-***`ejemplo1234567890`***), situado en la parte superior de la página, elija el ID del volumen que acaba de crear.
8. Elija Actions (Acciones), Attach Volume (Adjuntar volumen).
9. En la página Adjuntar volumen, en instancia, seleccione el ID de su instancia de Windows y, a continuación, elija Adjuntar volumen.
10. Haga que el nuevo volumen esté disponible para su uso siguiendo los pasos que se indican en Hacer que un volumen de Amazon EBS esté disponible para su uso.

> **Important**
>
> No inicialice el disco porque al hacerlo se eliminarán los datos existentes.

11. En Windows PowerShell, cambie a la nueva unidad de volumen. Empiece la actualización abriendo el volumen de contenido multimedia de instalación que ha adjuntado a la instancia.

a. Si va a actualizar a Windows Server 2016 o una versión posterior, ejecute lo siguiente:

```
.\setup.exe /auto upgrade /dynamicupdate disable
```

> **Note**
>
> La ejecución de setup.exe con la opción `/dynamicupdate` deshabilitada impide que Windows instale actualizaciones durante el proceso de actualización de Windows Server, ya que la instalación de actualizaciones durante la actualización puede provocar errores. Puede instalar actualizaciones con Windows Update una vez finalizada la actualización.

Si va a actualizar a una versión anterior de Windows Server, ejecute lo siguiente:

```
Sources\setup.exe
```

b. En Select the operating system you want to install (Seleccione el sistema operativo que desea instalar), seleccione el SKU de instalación completa para la instancia de Windows Server y elija Next (Siguiente).

c. En Which type of installation do you want? (¿Qué tipo de instalación desea?), elija Upgrade (Actualizar).

d. Complete el asistente.

El programa de instalación de Windows Server copia y procesa los archivos. Tras varios minutos, se cierra la sesión de escritorio remoto. El tiempo que tarda la actualización depende del número de aplicaciones y roles de servidor que se ejecuten en la instancia de Windows Server. El proceso de actualización podría tardar desde 40 minutos a varias horas. La instancia da error en la comprobación de estado 1 de 2 durante el proceso de actualización. Una vez finalizada la actualización, se superan las dos comprobaciones de estado. Puede consultar en el registro del sistema el resultado de la consola o utilizar las métricas de Amazon CloudWatch de la actividad del disco y la CPU para determinar si la actualización está progresando.

> **Note**
>
> Si actualiza a Windows Server 2019, una vez completada la actualización, puede cambiar manualmente el fondo del escritorio para quitar el nombre del sistema operativo anterior.

Si la instancia no ha superado ambas comprobaciones de estado tras varias horas, consulte Solución de problemas de una actualización en una instancia de Windows.

Tareas después de la actualización

1. Inicie sesión en la instancia para comenzar la actualización de .NET Framework y reinicie el sistema cuando se le indique.
2. Si aún no lo hizo en un paso anterior, instale el agente de EC2Launch v1 o EC2Launch v2. Para obtener más información, consulte Configurar una instancia de Windows utilizando EC2Launch y Configurar una instancia de Windows mediante EC2Launch v2.

3. Si actualizó a Windows Server 2012 R2, recomendamos que actualice los controladores PV a controladores AWS PV. Si ha actualizado en una instancia basada en Nitro, le recomendamos que instale o actualice los controladores NVME y ENA. Para obtener más información, consulte Windows Server 2012 R2, Instalar o actualizar controladores NVMe de AWS mediante PowerShell o Habilitar redes mejoradas en Windows.
4. Vuelva a habilitar el software antivirus y antispyware y los firewalls.

Cómo realizar una actualización automatizada en su instancia de Windows

Puede llevar a cabo una actualización automatizada de las instancias de Windows y SQL Server en AWS con manuales de procedimientos de AWS Systems Manager Automation.

Contenido

Servicios relacionados

Los siguientes servicios de AWS se utilizan en el proceso de actualización automatizado:

- AWS Systems Manager. AWS Systems Manager es una potente interfaz unificada para administrar de forma centralizada los recursos de AWS. Para obtener más información, consulte la Guía del usuario de AWS Systems Manager.
- El agente de AWS Systems Manager (SSM Agent) es el software de Amazon que se puede instalar y configurar en una instancia de Amazon EC2, en un servidor en las instalaciones o en una máquina virtual (VM). El SSM Agent posibilita que Systems Manager actualice, administre y configure estos recursos. El agente procesa las solicitudes del servicio de Systems Manager de la nube de AWS y, a continuación, las ejecuta como se especifica en la solicitud. Para obtener más información, consulte Usar el SSM Agent en la Guía del usuario de AWS Systems Manager.
- Manuales de procedimientos de AWS Systems Manager SSM. Un runbook de SSM define las acciones que Systems Manager realiza en las instancias administradas. Los manuales de procedimientos de SSM utilizan JavaScript Object Notation (JSON) o YAML, e incluyen los pasos y los parámetros que especifique. En este tema se utilizan dos manuales de procedimientos de SSM de Systems Manager para la automatización. Para obtener más información, consulte Referencia

del runbook de AWS Systems Manager Automation en la Guía del usuario de AWS Systems Manager.

Opciones de ejecución

Cuando seleccione Automation (Automatización) en la consola de Administrador de sistemas, seleccione Execute (Ejecutar). Después de seleccionar un documento Automation, se le solicita que elija una opción de ejecución de automatización. Puede elegir entre las siguientes opciones. En los pasos para las rutas indicados posteriormente en este tema, utilizamos la opción de ejecución simple.

Ejecución simple

Elija esta opción si desea actualizar una única instancia pero no desea pasar por todos los pasos de automatización para realizar una auditoría de los resultados. Esta opción se explica con mayor detalles en los pasos de actualización más adelante.

Rate control (Control de velocidad)

Elija esta opción si desea aplicar la actualización a más de una instancia. Define las opciones siguientes.

- Parámetro

  Esta configuración, que también se establece en la configuración de varias cuentas y regiones, define cómo se ramificará la automatización.
- Destinos

  Seleccione el destino al que desea aplicar la automatización. Este parámetro también se establece en la configuración de varias cuentas y regiones.
- Parameter Values (Valores de parámetro)

  Utilice los valores definidos en los parámetros de documento de automatización.
- Grupo de recursos

  En AWS, un recurso es una entidad con la que se puede trabajar. Entre los ejemplos se incluyen instancias de Amazon EC2, pilas de AWS CloudFormation o buckets de Amazon S3. Si trabaja con varios recursos, puede resultarle útil administrarlos como un grupo en lugar de transferirlos de un servicio de AWS a otro para cada tarea. En algunos casos, es posible que desee administrar

un gran número de recursos relacionados, como instancias de EC2 que componen una capa de aplicación. En este caso, es probable que tenga que llevar a cabo acciones por lotes en estos recursos a la vez.

- Etiquetas

  Las etiquetas le permiten clasificar los recursos de AWS de diversas maneras, por ejemplo, según su finalidad, propietario o entorno. Esta clasificación es útil cuando se tienen muchos recursos del mismo tipo. Puede identificar rápidamente un recurso específico según las etiquetas asignadas.

- Rate Control (Control de velocidad)

  El control de velocidad también se establece en la configuración de varias cuentas y regiones. Cuando se definen los parámetros de control de velocidad, defina a cuántos de la flota se aplica la automatización, bien por recuento de destino o por porcentaje de la flota.

Multi-Account and Region (Varias cuentas y regiones)

Además de los parámetros especificados en control de velocidad que se utilizan en la configuración de varias cuentas y regiones, hay dos configuraciones adicionales:

- Accounts and organizational units (OUs) [Cuentas y unidades organizativas (OU)]

  Especifique varias cuentas en las que desee ejecutar la automatización.

- Regiones de AWS

  Especifique varias Regiones de AWS en las que desea ejecutar la automatización.

Ejecución manual

Esta opción es similar a Simple execution (Ejecución simple), pero le permite pasar por cada paso de automatización y realizar una auditoría de los resultados.

Actualización de Windows Server

El manual de procedimientos de `AWSEC2-CloneInstanceAndUpgradeWindows` crea una Imagen de máquina de Amazon (AMI) desde una instancia de Windows Server en su cuenta y actualiza esta AMI a una versión compatible de su elección. Este proceso de varios pasos puede tardar hasta dos horas en completarse.

Hay dos AMI incluidas en el proceso de actualización automatizado:

- instancia en ejecución actual. La primera AMI es la instancia en ejecución actual, que no está actualizada. Esta AMI se utiliza para iniciar otra instancia para ejecutar la actualización in situ. Cuando el proceso está completo, esta AMI se elimina de su cuenta, a menos que solicite específicamente mantener la instancia original. Esta configuración se gestiona mediante el parámetro `KeepPreUpgradeImageBackUp` (el valor predeterminado es `false`, que significa que la AMI se elimina de forma predeterminada).
- AMI actualizada. Esta AMI es el resultado del proceso de automatización.

El resultado final es una AMI, que es la instancia actualizada de la AMI.

Cuando la actualización está completa, puede probar la funcionalidad de la aplicación al iniciar la nueva AMI en la Amazon VPC. Una vez realizadas las pruebas y antes de realizar otra actualización, programe el tiempo de inactividad de las aplicaciones antes de cambiar completamente a la instancia actualizada.

Requisitos previos

Para automatizar la actualización de Windows Server con documentos de AWS Systems Manager Automation, debe llevar a cabo las tareas siguientes:

- Crear un rol de IAM con las políticas de IAM especificadas para permitir a Systems Manager llevar a cabo tareas de automatización en sus instancias Amazon EC2 y verificar que cumple los requisitos previos para utilizar Systems Manager. Para obtener más información, consulte Creación de un rol para delegar permisos a un servicio de AWS en la Guía del usuario de AWS Identity and Access Management.
- Seleccione la opción para la que desea ejecutar la automatización. Las opciones para ejecución son Simple execution (Ejecución simple), Rate control (Control de velocidad), Multi-account and Region (Varias cuentas y regiones) y Manual execution (Ejecución manual). Para obtener más información sobre estas opciones, consulte Opciones de ejecución.
- Compruebe que SSM Agent esté instalado en su instancia. Para obtener más información, consulte Instalación y configuración de SSM Agent en instancias de Amazon EC2 para Windows Server.
- Windows PowerShell 3.0 o posterior debe estar instalado en la instancia.
- Para las instancias que están unidas a un dominio de Microsoft Active Directory, se recomienda especificar un `SubnetId` que no tenga conectividad con los controladores de dominio para evitar conflictos con nombres de host.

- La subred de la instancia debe tener conectividad saliente a Internet, lo que proporciona acceso a Servicios de AWS como Amazon S3 y acceso a la descarga de revisiones de Microsoft. Este requisito se cumple si la subred es pública y la instancia tiene una dirección IP pública, o si la subred es una subred privada con una ruta que envía el tráfico de Internet a un dispositivo de NAT público.
- Esta automatización funciona con instancias que ejecutan Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2016 y Windows Server 2019.
- Verifique que la instancia tiene 20 GB de espacio libre en el disco de arranque.
- Si la instancia no utiliza una licencia de Windows proporcionada por AWS, especifique un ID de instantánea de Amazon EBS que incluya los medios de instalación de Windows Server 2012 R2. Para ello:
  1. Compruebe que las instancias de Amazon EC2 ejecuten Windows Server 2012 o una versión posterior.
  2. Cree un volumen de Amazon EBS de 6 GB en la misma zona de disponibilidad en la que se ejecuta la instancia. Adjunte el volumen a la instancia. Móntelo, por ejemplo, como unidad D.
  3. Haga clic con el botón derecho del ratón en la ISO y móntela en una instancia como, por ejemplo, la unidad E.
  4. Copie el contenido de la ISO desde la unidad E:\ a la unidad D:\
  5. Cree una instantánea de Amazon EBS del volumen de 6 GB creado en el paso 2 anterior.

Límites de actualización de Windows Server

Esta automatización no admite la actualización de controladores de dominio de Windows, clústeres o sistemas operativos de escritorio de Windows. Además, esta automatización no admite instancias de Amazon EC2 para Windows Server con los siguientes roles instalados:

- Host de sesión de Escritorio remoto (RDSH)
- Agente de conexión a Escritorio remoto (RDCB)
- Host de virtualización de Escritorio remoto (RDVH)
- Acceso web de Escritorio remoto (RDWA)

Pasos para realizar una actualización automatizada de Windows Server

Siga estos pasos para actualizar la instancia de Windows Server mediante el runbook AWSEC2-CloneInstanceAndUpgradeWindows de automatización.

1. Abra Systems Manager desde AWS Management Console.
2. Desde el panel de navegación izquierdo, en Change Management (Administración de cambios), elija Automation(Automatización).
3. Elija Execute automation (Ejecutar automatización).
4. Busque el documento de automatización denominado `AWSEC2-CloneInstanceAndUpgradeWindows`.
5. Cuando aparezca el nombre del documento, selecciónelo. Cuando lo seleccione, aparecen los detalles del documento.
6. Elija Execute automation (Ejecutar automatización) para introducir los parámetros de este documento. Deje Simple execution (Ejecución simple) seleccionado al principio de la página.
7. Introduzca los parámetros solicitados en función del siguiente asesoramiento.

   - `InstanceID`

     Tipo: cadena

     (Requerido) La instancia que ejecuta Windows Server 2008 R2, 2012 R2, 2016 o 2019 con SSM Agent instalado.
   - `InstanceProfile`.

     Tipo: cadena

     (Obligatorio) El perfil de instancia de IAM. Este es el rol de IAM utilizado para ejecutar la automatización de Systems Manager frente a la instancia de Amazon EC2 y las AMI de AWS. Para obtener más información, consulte Crear un perfil de instancias de IAM para Systems Manager en la Guía del usuario de AWS Systems Manager.
   - `TargetWindowsVersion`

     Tipo: cadena

     (Obligatorio) Seleccionar la versión de Windows de destino.
   - `SubnetId`

     Tipo: cadena

     (Requerido) Esta es la subred para el proceso de actualización y donde reside su instancia de EC2 de origen. Verifique que la subred tenga conectividad saliente a los servicios de AWS, incluido Amazon S3, y también a Microsoft (para descargar parches).

- `KeepPreUpgradedBackUp`

  Tipo: cadena

  (Opcional) Si este parámetro se establece en `true`, la automatización conserva la imagen creada desde la instancia. El valor predeterminado es `false`.

- `RebootInstanceBeforeTakingImage`

  Tipo: cadena

  (Opcional) El valor predeterminado es `false` (sin reinicio). Si este parámetro se establece en `true`, Administrador de sistemas reinicia la instancia antes de crear una AMI para la actualización.

8. Después de introducir los parámetros, elija Execute (Ejecutar). Cuando se inicia la automatización, puede monitorizar el progreso de ejecución.
9. Cuando se complete la automatización, verá el ID de la AMI. Puede iniciar la AMI para verificar que el sistema operativo Windows está actualizado.

> **Note**
>
> No es necesario que la automatización ejecute todos los pasos. Los pasos son condicionales en función del comportamiento de la automatización y la instancia. Es posible que Systems Manager salte algunos pasos que no sean obligatorios. Además, algunos de ellos pueden agotar el tiempo de espera. Systems Manager intenta actualizar e instalar todos los parches más recientes. En ocasiones, sin embargo, los parches agotan el tiempo de espera en función de una configuración de tiempo de espera definible para el paso dado. Cuando esto ocurre, la automatización de Systems Manager continúa al paso siguiente para asegurarse de que el sistema operativo interno se actualice a la versión de Windows Server de destino.

10. Una vez completada la automatización, puede iniciar una instancia de Amazon EC2 utilizando el ID de AMI para revisar su actualización. Para obtener más información sobre la creación de una instancia de Amazon EC2 desde una AMI de AWS, consulte ¿Cómo puedo lanzar una instancia de EC2 desde una AMI personalizada?

Actualización de SQL Server

El script de `AWSEC2-CloneInstanceAndUpgradeSQLServer` crea una AMI desde una instancia de Amazon EC2 que ejecuta SQL Server en la cuenta y, a continuación, actualiza la AMI a una versión posterior de SQL Server. Este proceso de varios pasos puede tardar hasta dos horas en completarse.

En este flujo de trabajo, la automatización crea una AMI desde la instancia y, a continuación, inicia la nueva AMI en la subred que proporcione. A continuación, la automatización realiza una actualización in situ de SQL Server. Después de la actualización, la automatización crea una nueva AMI antes de terminar la instancia actualizada.

Hay dos AMI incluidas en el proceso de actualización automatizado:

- instancia en ejecución actual. La primera AMI es la instancia en ejecución actual, que no está actualizada. Esta AMI se utiliza para iniciar otra instancia para ejecutar la actualización in situ. Cuando el proceso está completo, esta AMI se elimina de su cuenta, a menos que solicite específicamente mantener la instancia original. Esta configuración se gestiona mediante el parámetro `KeepPreUpgradeImageBackUp` (el valor predeterminado es `false`, que significa que la AMI se elimina de forma predeterminada).
- AMI actualizada. Esta AMI es el resultado del proceso de automatización.

El resultado final es una AMI, que es la instancia actualizada de la AMI.

Cuando la actualización está completa, puede probar la funcionalidad de la aplicación al iniciar la nueva AMI en la Amazon VPC. Una vez realizadas las pruebas y antes de realizar otra actualización, programe el tiempo de inactividad de las aplicaciones antes de cambiar completamente a la instancia actualizada.

Requisitos previos

Para automatizar la actualización de SQL Server con documentos de AWS Systems Manager Automation, debe llevar a cabo las tareas siguientes:

- Crear un rol de IAM con las políticas de IAM especificadas para permitir a Systems Manager llevar a cabo tareas de automatización en sus instancias Amazon EC2 y verificar que cumple los requisitos previos para utilizar Systems Manager. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la AWS Identity and Access ManagementGuía del usuario.

- Seleccione la opción para la que desea ejecutar la automatización. Las opciones para ejecución son Simple execution (Ejecución simple), Rate control (Control de velocidad), Multi-account and Region (Varias cuentas y regiones) y Manual execution (Ejecución manual). Para obtener más información sobre estas opciones, consulte Opciones de ejecución.
- La instancia de Amazon EC2 debe utilizar Windows Server 2008 R2 o posterior y SQL Server 2008 o posterior.
- Compruebe que SSM Agent esté instalado en su instancia. Para obtener más información, consulte Uso de SSM Agent en instancias de Amazon EC2 para Windows Server.
- Verifique que la instancia tiene espacio de disco suficiente:
  - Si va a actualizar de Windows Server 2008 R2 a 2012 R2, o de Windows Server 2012 R2 a un sistema operativo posterior, compruebe que tenga 20 GB de espacio libre en el disco de arranque de la instancia.
  - Si va a actualizar de Windows Server 2008 R2 a una versión 2016 o posterior, compruebe que la instancia tenga 40 GB de espacio libre en el disco de arranque.
- Para las instancias que utilizan una versión Bring Your Own License (BYOL) de SQL Server, se aplican los siguientes requisitos previos adicionales:
  - Proporcione un ID de instantánea de Amazon EBS que incluya medios de instalación de destino de SQL Server. Para ello:
    1. Compruebe que las instancias de Amazon EC2 ejecuten Windows Server 2008 R2 o una versión posterior.
    2. Cree un volumen de Amazon EBS de 6 GB en la misma zona de disponibilidad en la que se ejecuta la instancia. Adjunte el volumen a la instancia. Móntelo, por ejemplo, como unidad D.
    3. Haga clic con el botón derecho del ratón en la ISO y móntela en una instancia como, por ejemplo, la unidad E.
    4. Copie el contenido de la ISO desde la unidad E:\ a la unidad D:\
    5. Cree una instantánea de Amazon EBS del volumen de 6 GB creado en el paso 2.

Limitaciones de actualización automatizada de SQL Server

Al utilizar el comando del runbook AWSEC2-CloneInstanceAndUpgradeSQLServer para realizar una actualización automatizada, se aplican las siguientes limitaciones:

- La actualización solo se puede realizar en un SQL Server mediante la autenticación de Windows.

- Verifique que no exista ninguna actualización de parches de seguridad pendiente en las instancias. Abra Control Panel (Panel de control) y elija Check for updates (Buscar actualizaciones).
- No se admiten las implementaciones de SQL Server en HA y el modo de duplicación.

Pasos para realizar una actualización automatizada de SQL Server

Siga estos pasos para actualizar su SQL Server mediante el runbook AWSEC2-CloneInstanceAndUpgradeSQLServer de automatización.

1. Si no lo ha hecho aún, descargue el archivo .iso de SQL Server 2016 y móntelo en el servidor de origen.
2. Una vez que el archivo .iso se ha montado, copie todos los archivos de componentes y colóquelos en cualquier volumen de su elección.
3. Tome una instantánea de Amazon EBS del volumen y copie el ID de instantánea en un portapapeles para utilizarlo posteriormente. Para obtener más información, consulte Creación de instantáneas de Amazon EBS en la Guía del usuario de Amazon EBS.
4. Adjunte el perfil de instancia a la instancia de Amazon EC2 de origen. Esto permite a Systems Manager comunicarse con la instancia de EC2 y ejecutar comandos en esta después de agregarla al servicio de AWS Systems Manager. En este ejemplo, denominamos el rol `SSM-EC2-Profile-Role` con la política `AmazonSSMManagedInstanceCore` asociada al rol. Consulte Creación de un perfil de instancias de IAM para Systems Manager en la Guía del usuario de AWS Systems Manager.
5. En la consola de AWS Systems Manager, en el panel de navegación izquierdo, elija Managed Instances (instancias administradas). Verifique que su instancia de EC2 esté en la lista de instancias administradas. Si no ve su instancia después de unos minutos, consulte ¿Dónde están mis instancias? en la Guía del usuario de AWS Systems Manager.
6. En el panel de navegación izquierdo, en Change Management (Administración de cambios), elija Automation (Automatización).
7. Elija Execute automation (Ejecutar automatización).
8. Busque el documento de automatización denominado `AWSEC2-CloneInstanceAndUpgradeSQLServer`.
9. Elija el documento de SSM `AWSEC2-CloneInstanceAndUpgradeSQLServer` y elija Next (Siguiente).
10. Asegúrese de haber seleccionado la opción Simple execution (Ejecución simple).
11. Introduzca los parámetros solicitados en función del siguiente asesoramiento.

- `InstanceId`

  Tipo: cadena

  (Obligatorio) la instancia que ejecuta SQL Server 2008 R2 (o posterior).

- `IamInstanceProfile`

  Tipo: cadena

  (Obligatorio) El perfil de instancia de IAM.

- `SQLServerSnapshotId`

  Tipo: cadena

  (Obligatorio) El ID de instantánea para los medios de instalación de SQL Server de destino. Este parámetro no es necesario para las instancias con licencia incluida de SQL Server.

- `SubnetId`

  Tipo: cadena

  (Requerido) Esta es la subred para el proceso de actualización y donde reside su instancia de EC2 de origen. Verifique que la subred tenga conectividad saliente a los servicios de AWS, incluido Amazon S3, y también a Microsoft (para descargar parches).

- `KeepPreUpgradedBackUp`

  Tipo: cadena

  (Opcional) Si este parámetro se establece en `true`, la automatización conserva la imagen creada desde la instancia. El valor predeterminado es `false`.

- `RebootInstanceBeforeTakingImage`

  Tipo: cadena

  (Opcional) El valor predeterminado es `false` (sin reinicio). Si este parámetro se establece en `true`, Administrador de sistemas reinicia la instancia antes de crear una AMI para la actualización.

- `TargetSQLVersion`

  Tipo: cadena

(Opcional) La versión de SQL Server de destino. El valor predeterminado es `2016`.

12. Después de introducir los parámetros, elija Execute (Ejecutar). Cuando se inicia la automatización, puede monitorizar el progreso de ejecución.
13. Cuando Execution Status (Estado de ejecución) muestre Success (Éxito), expanda Outputs (Salidas) para ver la información de la AMI. Puede utilizar el ID de la AMI para iniciar su instancia de SQL Server para la VPC que elija.
14. Abra la consola de Amazon EC2. En el panel de navegación izquierdo, elija AMIs. Debería ver la nueva AMI.
15. Para verificar que la nueva versión de SQL Server se ha instalado correctamente, elija la nueva AMI y elija Launch (iniciar).
16. Elija el tipo de instancia que desea para la AMI, la VPC y la subred en la que la desea implementar, así como el almacenamiento que desea utilizar. Dado que está iniciando la nueva instancia desde una AMI, los volúmenes se presentan de forma opcional para incluirlos en la nueva instancia de EC2 que está iniciando. Puede eliminar cualquiera de estos volúmenes o puede añadir volúmenes.
17. Añada una etiqueta para ayudar a identificar la instancia.
18. Añada el grupo o grupos de seguridad a la instancia.
19. Elija Launch Instance.
20. Elija el nombre de etiqueta para la instancia y seleccione Connect (Conectar) en la lista desplegable Actions (Acciones).
21. Verifique que la nueva versión de SQL Server sea el motor de base de datos en la nueva instancia.

Migración de una instancia de Windows a un tipo de instancia de generación actual

Las AMI de Windows de AWS se configuran con los ajustes predeterminados que utilizan los medios de instalación de Microsoft, con algunas personalizaciones. Las personalizaciones incluyen controladores y configuraciones compatibles con los tipos de instancia de última generación, que son instancias integradas en el AWS Nitro System, como, por ejemplo una M5 o una C5.

En el momento de migrar a instancias basadas en Nitro, incluidas las instancias bare metal, le recomendamos que siga los pasos de este tema en los siguientes casos:

- Si está iniciando instancias desde AMI de Windows personalizadas
- Si está iniciando instancias desde AMI de Windows proporcionadas por Amazon creadas antes de agosto de 2018

Para obtener más información, consulte Actualización de Amazon EC2: otros tipos de instancias, el sistema Nitro y opciones de CPU.

> **Note**
>
> Los siguientes procedimientos de migración se pueden llevar a cabo en la versión 2008 R2 de Windows Server y versiones posteriores. Para migrar instancias de Linux a los tipos de instancias de última generación, consulte the section called “Cambie el tipo de instancia”.

Contenido

> **Note**
>
> También puede utilizar el documento de automatización `AWSSupport-UpgradeWindowsAWSDrivers` para automatizar los procedimientos descritos en la parte 1, la parte 2 y la parte 3. Si decide utilizar el procedimiento automatizado, consulte (Alternativa) Actualizar los controladores PV, ENA y NVMe de AWS utilizando AWS Systems Manager y continúe con la parte 4 y la parte 5.

Antes de empezar

En este procedimiento, se asume que actualmente se está ejecutando un tipo de instancia basada en Xen de una generación anterior, como M4 o C4, y que se está migrando a una instancia integrada en el AWS Nitro System.

Debe usar PowerShell, versión 3.0 o posterior, para realizar correctamente la actualización.

> **Note**
>
> Al migrar a las instancias de última generación, la configuración de la IP estática o de la red DNS personalizada en la ENI existente puede perderse pues la instancia tomará los valores predeterminados de un nuevo dispositivo Enhanced Networking Adapter.

Antes de seguir los pasos que se indican en este procedimiento, le recomendamos que cree una copia de seguridad de la instancia. En la consola de EC2, elija la instancia que se va a migrar, abra el menú contextual (con el botón derecho) y elija Instance State (Estado de la instancia), Stop (Detener).

> **Warning**
>
> Cuando detiene una instancia, se borran los datos contenidos en todos los volúmenes de almacén de instancias. Con el fin de conservar los datos de los volúmenes de almacén de instancias, asegúrese de realizar una copia de seguridad de los datos en un almacenamiento persistente.

Abra el menú contextual de la instancia (haga clic con el botón derecho) en la consola de EC2 y seleccione Image (Imagen) y Create Image (Crear imagen).

> **Note**
>
> Las secciones 4 y 5 de estas instrucciones pueden completarse después de migrar o cambiar el tipo de instancia a otro de última generación. No obstante, es recomendable que siga estos pasos antes de realizar la migración si el destino es un tipo de instancia Bare Metal.

Parte 1: instalación y actualización de controladores AWS PV

Aunque los controladores AWS PV no se utilizan en el sistema Nitro, sigue siendo conveniente actualizarlos si se utilizan versiones anteriores de Citrix PV o AWS PV. Los últimos controladores PV de AWS resuelven errores de las versiones anteriores que podrían manifestarse cuando trabaje en el sistema Nitro o si necesita migrar de nuevo a una instancia basada en Xen. Es recomendable que actualice siempre los controladores más recientes de las instancias de Windows de AWS.

Utilice los siguientes procedimientos para llevar a cabo una actualización in situ de los controladores AWS PV o para actualizar los controladores Citrix PV a AWS PV en Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 o Windows Server 2019. Para obtener más información, consulte Actualizar controladores PV en instancias de Windows.

Para actualizar un controlador de dominio, consulte Actualice un controlador de dominio (actualización de AWS PV).

Para realizar una actualización de los controladores AWS PV o a los mismos.

1. Conéctese a la instancia mediante el Escritorio remoto y prepare la instancia para la actualización. Desconecte los discos que no son del sistema antes de llevar a cabo la actualización. Este paso no es obligatorio si se está haciendo una actualización in situ de los controladores AWS PV. Establezca los servicios no esenciales en inicio Manual en la consola de servicios.
2. Descargue el último paquete del controlador en la instancia.
3. Extraiga el contenido de la carpeta y ejecute `AWSPVDriverSetup.msi`.

Después de ejecutar MSI, la instancia vuelve a arrancar automáticamente y actualiza el controlador. Es posible que la instancia no esté disponible hasta pasados unos 15 minutos como máximo.

Una vez finalizada la actualización y cuando la instancia haya superado las dos comprobaciones de estado en la consola de Amazon EC2, conéctese a la instancia mediante el Escritorio remoto y compruebe que el nuevo controlador se ha instalado. En Device Manager (Administrador de dispositivos), en Storage Controllers (Controladores de almacenamiento), localice PV Storage Host Adapter (Adaptador de host de almacenamiento de AWS). Verifique que la versión del controlador es la misma versión que la última enumerada en la tabla del historial de versiones del controlador. Para obtener más información, consulte Historial de paquetes de controladores AWS PV.

Parte 2: instalar y actualizar ENA

Actualice al último controlador de Elastic Network Adapter para garantizar la compatibilidad de todas las características de red. Si ha iniciado la instancia y no tiene habilitadas las redes mejoradas, debe descargar e instalar el controlador del adaptador de red necesario en la instancia. A continuación, establezca el atributo enaSupport de la instancia para activar las redes mejoradas. Solo puede habilitar este atributo en los tipos de instancias admitidos y solo si está instalado el controlador de ENA. Para obtener más información, consulte Habilitación de las redes mejoradas con Elastic Network Adapter (ENA) en las instancias EC2.

1. Descargue el controlador más reciente en la instancia.
2. Extraiga el archivo zip.
3. Para instalar el controlador, ejecute el script `install.ps1` de PowerShell en la carpeta extraída.

   > **Note**
   >
   > Para evitar errores de instalación, ejecute el script `install.ps1` como administrador.

4. Compruebe si la AMI tiene activado el atributo enaSupport. De no ser así, siga los pasos que se indican en Habilitación de las redes mejoradas con Elastic Network Adapter (ENA) en las instancias EC2.

Parte 3: actualización de controladores NVMe de AWS

Los controladores NVMe de AWS se usan para interactuar con los volúmenes del almacén de instancias de Amazon EBS y SSD que se exponen como dispositivo de bloques NVMe en el sistema Nitro para mejorar el rendimiento.

> **Important**
>
> Las siguientes instrucciones se han modificado expresamente para cuando se instale o actualice AWS NVMe en una instancia de una generación anterior con la intención de migrar dicha instancia a un tipo de instancia de última generación.

1. Descargue el último paquete del controlador en la instancia.

2. Extraiga el archivo zip.
3. Instale el controlador ejecutando `dpinst.exe`.
4. Abra una sesión de PowerShell y ejecute el siguiente comando:

```
PS C:\> start rundll32.exe sppnp.dll,Sysprep_Generalize_Pnp -wait
```

> **Note**
>
> Para aplicar el comando, debe ejecutar la sesión de PowerShell como administrador. Las versiones de PowerShell (x86) producirán un error.
> Este comando solo ejecuta sysprep en los controladores de dispositivos. No ejecuta la preparación de sysprep completa.

5. En Windows Server 2008 R2 y en Windows Server 2012, apague la instancia, cambie el tipo de instancia por uno de última generación, reiníciela y continúe con la sección 4. Si vuelve a iniciar la instancia en un tipo de una generación anterior antes de migrarla a un tipo de última generación, no arrancará. Para las demás AMI de Windows admitidas, puede cambiar el tipo de instancia en cualquier momento después de ejecutar sysprep en el dispositivo.

Sección 4: actualizar EC2Config y EC2Launch

En las instancias de Windows, las utilidades EC2Config y EC2Launch más recientes proporcionarán información y funcionalidades adicionales cuando se ejecuten en el sistema Nitro, incluso en las instancias de EC2 Bare Metal (sin sistema operativo). De forma predeterminada, el servicio EC2Config está incluido en las AMI anteriores a Windows Server 2016. En las AMI de Windows Server 2016 y versiones posteriores, EC2Launch sustituye a EC2Config.

Cuando se actualizan los servicios EC2Config y EC2Launch, las nuevas AMI de Windows procedentes de AWS contienen la última versión del servicio. No obstante, necesitará actualizar sus propias AMI e instancias de Windows con la versión más reciente de EC2Config y EC2Launch.

Para instalar o actualizar EC2Config

1. Descargue y descomprima el instalador de EC2Config.
2. Ejecute `EC2Install.exe`. Para obtener una lista completa de opciones, ejecute `EC2Install` con la opción `/?`. De forma predeterminada, el proceso de configuración muestra preguntas. Para ejecutar el comando sin este tipo de preguntas, utilice la opción `/quiet`.

Para obtener más información, consulte Instalar la versión más reciente de EC2Config.

Para instalar o actualizar EC2Launch

1. Si ya ha instalado y configurado EC2Launch en una instancia, realice una copia de seguridad del archivo de configuración de EC2Launch. Durante el proceso de instalación, no se conservan los cambios realizados en este archivo. De forma predeterminada, el archivo se ubica en el directorio `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.
2. Descargue EC2-Windows-Launch.zip en un directorio de la instancia.
3. Descargue install.ps1 en el mismo directorio en que ha descargado `EC2-Windows-Launch.zip`.
4. Ejecute `install.ps1`.

   > **Note**
   >
   > Para evitar errores de instalación, ejecute el script `install.ps1` como administrador.

5. Si ha realizado una copia de seguridad del archivo de configuración de EC2Launch, cópielo en el directorio `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.

Para obtener más información, consulte Configurar una instancia de Windows utilizando EC2Launch.

Parte 5: instalar el controlador del puerto serie para las instancias bare metal

El tipo de instancia `i3.metal` utiliza un dispositivo serie basado en PCI en vez de un dispositivo serie basado en puerto de E/S. Las últimas AMI de Windows utilizan automáticamente el dispositivo serie basado en PCI y tienen instalado el controlador del puerto serie. En caso de que no utilice una instancia iniciada desde una AMI de Windows proporcionada por Amazon con fecha igual o posterior al 11/04/2018, deberá instalar el controlador del puerto serie si quiere habilitar el dispositivo serie para características de EC2 como la generación de contraseñas y la salida de la consola. Las utilidades EC2Config y EC2Launch más recientes también son compatibles con i3.metal y proporcionan funciones adicionales. Siga los pasos de la parte 4, si aún no lo ha hecho.

Para instalar el controlador del puerto serie

1. Descargue el paquete del controlador del puerto serie en la instancia.
2. Extraiga el contenido de la carpeta, abra el menú contextual (con el botón derecho) para `aws_ser.INF` y elija “install” (Instalar).

3. Elija Okay (Aceptar).

Parte 6: actualizar la configuración de la administración de energía

La siguiente actualización de la configuración de la administración de energía establecerá que las pantallas no se apaguen nunca, lo que permite cierres apropiados del SO en el sistema Nitro. Todas las AMI de Windows proporcionadas por Amazon a partir del 28 de noviembre de 2018 ya incluyen esta configuración predeterminada.

1. Abra un símbolo del sistema o una sesión de PowerShell.
2. Ejecute los comandos siguientes:

```
powercfg /setacvalueindex 381b4222-f694-41f0-9685-ff5bb260df2e 7516b95f-
f776-4464-8c53-06167f40cc99 3c0bc021-c8a8-4e07-a973-6b14cbcb2b7e 0
powercfg /setacvalueindex 8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c 7516b95f-
f776-4464-8c53-06167f40cc99 3c0bc021-c8a8-4e07-a973-6b14cbcb2b7e 0
powercfg /setacvalueindex a1841308-3541-4fab-bc81-f71556f20b4a 7516b95f-
f776-4464-8c53-06167f40cc99 3c0bc021-c8a8-4e07-a973-6b14cbcb2b7e 0
```

Parte 7: actualizar los controladores del chipset de Intel para nuevos tipos de instancias

Los tipos de instancias `u-6tb1.metal`, `u-9tb1.metal` y `u-12tb1.metal` utilizan un hardware que necesita unos controladores de chipset que no estaban instalados en las AMI de Windows. Si no está utilizando una instancia iniciada desde una AMI de Windows proporcionada por Amazon con fecha del 19.11.2018 o una fecha posterior, debe instalar los controladores utilizando Intel Chipset INF Utility.

Para instalar los controladores del chipset

1. Descargue la utilidad del chipset en la instancia.
2. Extraiga los archivos.
3. Ejecute `SetupChipset.exe`.
4. Acepte el contrato de licencia de software de Intel e instale los controladores del chipset.
5. Reinicie la instancia.

(Alternativa) Actualizar los controladores PV, ENA y NVMe de AWS utilizando AWS Systems Manager

El documento de automatización `AWSSupport-UpgradeWindowsAWSDrivers` automatiza los pasos descritos en la parte 1, la parte 2 y la parte 3. Este método también permite reparar una instancia en la que no se han podido realizar las actualizaciones de los controladores.

El documento de automatización `AWSSupport-UpgradeWindowsAWSDrivers` actualiza o repara controladores de AWS de almacenamiento y de red en la instancia de EC2 especificada. El documento intenta instalar la versión más reciente de los controladores de AWS online llamando al agente de AWS Systems Manager (SSM Agent). Si el SSM Agent no responde, el documento puede llevar a cabo una instalación sin conexión de los controladores de AWS si se especifica de forma explícita.

> **Note**
>
> Este procedimiento producirá un error en un controlador de dominio. Para actualizar los controladores en un controlador de dominio, consulte Actualice un controlador de dominio (actualización de AWS PV).

Para actualizar de forma automática los controladores AWS PV, ENA y NVMe que utilizan AWS Systems Manager

1. Abra la consola de Administrador de sistemas en https://console.aws.amazon.com/systems-manager.
2. Elija Automation (Automatización), Execute Automation (Ejecutar automatización).
3. Busque y seleccione el documento de automatización AWSSupport-UpgradeWindowsAWSDrivers y, a continuación, seleccione Ejecutar automatización.
4. En la sección Parámetros de entrada, configure las siguientes opciones:

   ID de instancia

   Introduzca el ID único de la instancia que se va a actualizar.

   AllowOffline

   (Opcional) Elija una de las siguientes opciones:

- `True` — elija esta opción para realizar una instalación sin conexión. La instancia se detiene y se reinicia durante el proceso de actualización.

  > **Warning**
  >
  > Cuando detiene una instancia, se borran los datos contenidos en todos los volúmenes de almacén de instancias. Con el fin de conservar los datos de los volúmenes de almacén de instancias, asegúrese de realizar una copia de seguridad de los datos en un almacenamiento persistente.

- `False` — (predeterminada) deje esta opción seleccionada para realizar una instalación online. La instancia se reinicia durante el proceso de actualización.

  > **Important**
  >
  > Las actualizaciones online y sin conexión crean una AMI antes de intentar realizar las operaciones de actualización. La AMI se conserva una vez terminada la automatización. Proteja el acceso a la AMI o elimínela si ya no la necesita.

SubnetId

(Opcional) Escriba uno de los siguientes valores:

- `SelectedInstanceSubnet` — (predeterminado) el proceso de actualización inicia la instancia auxiliar en la misma subred que la instancia que se va a actualizar. La subred debe permitir la comunicación con los puntos de enlace de Administrador de sistemas (`ssm.*`).
- `CreateNewVPC` — el proceso de actualización inicia la instancia auxiliar en una VPC nueva. Utilice esta opción si no está seguro de si la subred de la instancia de destino permite la comunicación con los puntos de enlace de `ssm.*`. El usuario debe tener permiso para crear una VPC.
- Un ID de subred específico — especifique el ID de una subred específica en la que desee iniciar la instancia auxiliar. La subred debe estar en la misma zona de disponibilidad que la instancia que se va a actualizar y debe permitir la comunicación con los puntos de enlace de `ssm.*`.

5. Elija Ejecutar.

6. Deje que finalice la actualización. Las actualizaciones online pueden tardar hasta 10 minutos en finalizar, frente a los 25 minutos de las actualizaciones sin conexión.

Migración de una instancia de Windows a tipos de instancias Xen desde Nitro

En el siguiente procedimiento se asume que se está ejecutando actualmente en un tipo de instancia basada en Nitro y que se está migrando a una instancia basada en el sistema Xen, como M4 o C4. Para ver las especificaciones sobre los tipos de instancias, consulte la Guía de tipos de instancias de Amazon EC2. Realice los siguientes pasos antes de la migración para evitar errores durante el proceso de arranque.

Cómo migrar de Nitro a Xen

1. Haga una copia de seguridad de sus datos.
2. Compruebe que su política de SAN de Windows permite que los volúmenes de almacenamiento que no sean raíz se conecten a Internet.
3. Los controladores AWS PV deben instalarse y actualizarse en una instancia Nitro antes de migrar a una instancia Xen. Para obtener información sobre los pasos para instalar y actualizar los controladores AWS PV, consulte Parte 1: instalación y actualización de controladores AWS PV.
4. Actualice a la versión EC2Launch v2 más reciente. Para ver los pasos, consulte Migrar a EC2Launch v2.
5. Abra una sesión de PowerShell y ejecute el siguiente comando como administrador para ejecutar sysprep en los controladores de dispositivos. La ejecución de sysprep garantiza que los controladores de almacenamiento de arranque temprano necesarios para arrancar en instancias Xen se registren de forma correcta en Windows.

   > **Note**
   >
   > Ejecutar el comando con las versiones de PowerShell (x86) producirá un error. Este comando agrega solo los controladores de dispositivos críticos de arranque a la base de datos de dispositivos críticos. No ejecuta la preparación de sysprep completa.

   ```
   Start-Process rundll32.exe sppnp.dll,Sysprep_Generalize_Pnp -wait
   ```

6. Realice la migración a un tipo de instancia Xen cuando se complete el proceso de sysprep.

Asistente de redefinición de la plataforma de Windows a Linux para las bases de datos de Microsoft SQL Server

Para obtener información sobre la redefinición de la plataforma de las bases de datos de Microsoft SQL Server de Windows a Linux, consulte Asistente de redefinición de la plataforma de Windows a Linux para las bases de datos de Microsoft SQL Server en la Guía del usuario de Microsoft SQL Server en Amazon EC2.

Solución de problemas de una actualización en una instancia de Windows

AWS ofrece soporte para las actualizaciones con problemas con Upgrade Helper Service, una utilidad de AWS que ayuda a realizar actualizaciones in situ con controladores Citrix PV.

Tras la actualización, la instancia podría experimentar temporalmente un uso de la CPU superior a la media, mientras el servicio .NET Runtime Optimization optimiza .NET framework. Este es el comportamiento esperado.

Si la instancia no ha superado ambas comprobaciones de estado tras varias horas, compruebe lo que se indica a continuación.

- Si ha actualizado a Windows Server 2008 y ambas comprobaciones de estado dan error tras varias horas, puede que la actualización no se haya realizado con éxito y puede presentar la indicación Click OK (Haga clic en Aceptar) para confirmar la restauración. Puesto que no se puede obtener acceso a la consola en este estado, no hay forma de hacer clic en el botón. Para solucionarlo, vuelva a arrancar mediante la API o la consola de Amazon EC2. El nuevo arranque tarda diez minutos o más en iniciarse. La instancia podría estar disponible tras 25 minutos.
- Elimine del servidor las aplicaciones o los roles de servidor e inténtelo de nuevo.

Si la instancia no supera ambas comprobaciones de estado tras eliminar del servidor las aplicaciones o los roles del servidor, realice lo que se indica a continuación.

- Detenga la instancia y adjunte el volumen raíz a otra instancia. Para obtener más información, consulte la descripción acerca de cómo detener y adjuntar el volumen raíz a otra instancia en "Waiting for the metadata service".
- Analice los archivos de registro y los registros de eventos de Windows Setup para detectar si hay errores.

Si tiene otros problemas con la actualización o la migración de un sistema operativo, recomendamos leer los artículos disponibles en Antes de iniciar una actualización in situ.

Flota de EC2 y flota de spot

La flota de EC2 y la flota de spot están diseñadas para ser una forma útil de iniciar una flota (o grupo) de instancias con AWS. Cada instancia en una flota se basa en una plantilla de inicio o en un conjunto de parámetros de inicio que debe configurar manualmente al iniciarla.

Las flotas ofrecen las siguientes características y beneficios. Estos beneficios le permiten maximizar los ahorros de costos y optimizar la disponibilidad y el rendimiento al ejecutar aplicaciones en varias instancias de EC2.

Varios tipos de instancia y opciones de compra

: En una sola llamada a la API, una flota puede iniciar varios tipos de instancias y opciones de compra (instancias de spot y bajo demanda), lo que permite optimizar los costos mediante el uso de instancias de spot. También puede aprovechar los descuentos de instancia reservada y Savings Plan si los utiliza junto con las instancias bajo demanda de la flota.

Distribución de instancias entre zonas de disponibilidad

: Una flota intenta distribuir las instancias de manera uniforme en varias zonas de disponibilidad para obtener una alta disponibilidad. Esto proporciona resiliencia en caso de que una zona de disponibilidad deje de estar disponible.

Sustitución automática de instancias de spot

: Si su flota incluye instancias de spot, puede solicitar automáticamente la sustitución de la capacidad de spot si sus instancias de spot se ven interrumpidas o se deterioran debido a un cambio en el estado de la instancia. Mediante el reequilibrio de capacidad, una flota también puede monitorear y reemplazar de manera proactiva las instancias de spot que corren un riesgo elevado de interrupción.

La flota de EC2 es una buena opción si necesita flexibilidad para administrar aspectos del ciclo de vida de las instancias o los mecanismos de escalado. También puede usar la flota de spot, pero no es recomendable hacerlo porque es una API antigua sin inversión planificada. Sin embargo, si ya usa una flota de spot, puede seguir usándola. Las flotas de spot y de EC2 ofrecen la misma funcionalidad básica.

> **Tip**
>
> Como práctica recomendada general, se sugiere iniciar flotas de instancias de spot y bajo demanda con Amazon EC2 Auto Scaling, ya que proporciona características adicionales que puede usar para administrar su flota. La lista de características adicionales incluye la sustitución automática de las comprobaciones de estado para las instancias de spot y bajo demanda, las comprobaciones de estado basadas en las aplicaciones y una integración con Elastic Load Balancing para garantizar una distribución uniforme del tráfico de las aplicaciones a las instancias en buen estado. También puede utilizar grupos de escalado automático cuando utilice servicios de AWS como Amazon ECS, Amazon EKS (grupos de nodos autoadministrados) y Amazon VPC Lattice. Para obtener más información, consulte la Guía del usuario de Amazon EC2 Auto Scaling.

Temas

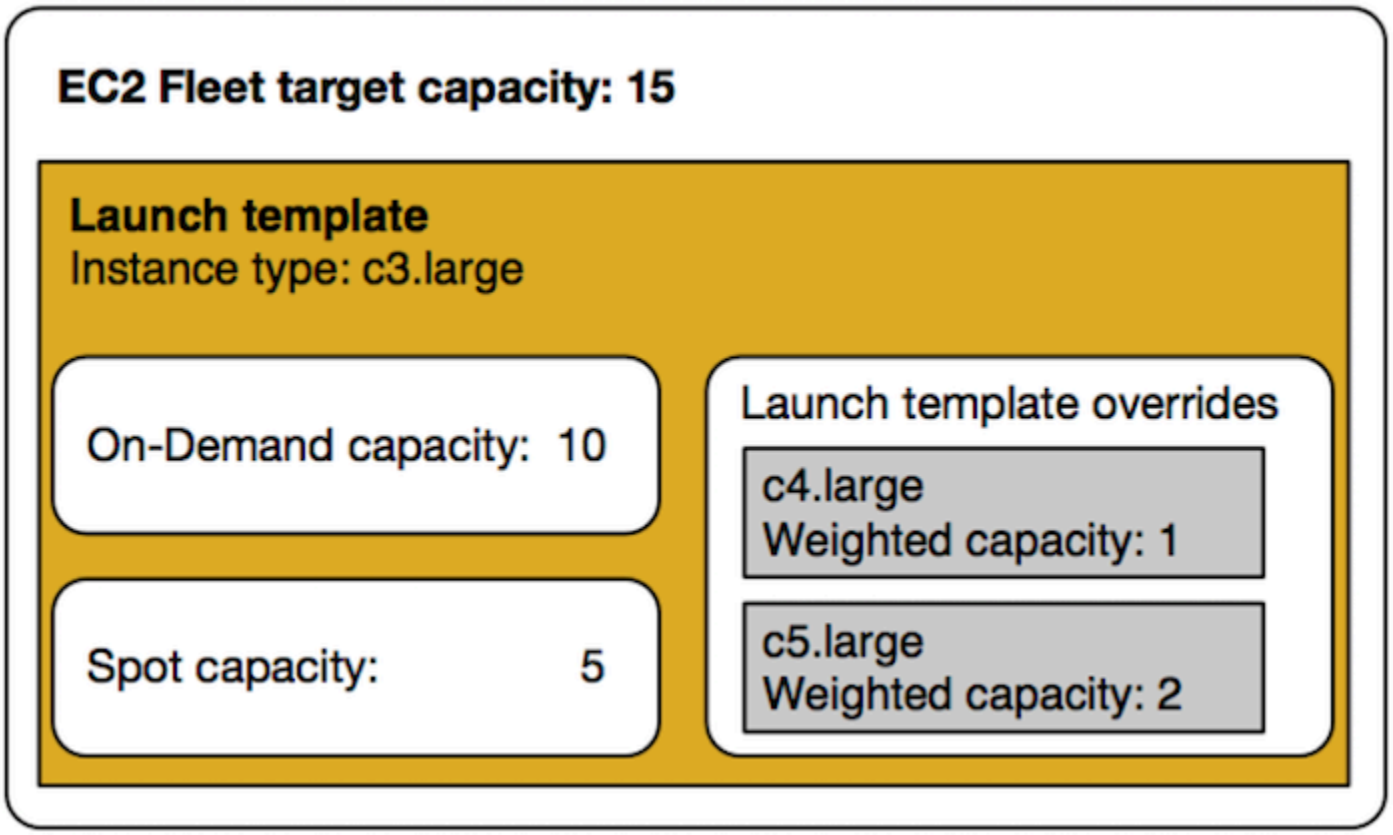
Flota de EC2

Una flota de EC2 contiene la información de configuración para iniciar una flota de instancias. En una sola llamada a la API, una flota puede iniciar varios tipos de instancias en varias zonas de disponibilidad, mediante el uso en conjunto de las opciones de instancia de spot, instancia bajo demanda, instancia reservada y Savings Plan. Con una flota de EC2, puede:

- Definir los objetivos de capacidad de spot y bajo demanda independientes y la cantidad máxima que está dispuesto a pagar por hora.
- Especificar los tipos de instancias que funcionan mejor con sus aplicaciones.
- Establecer cómo debe Amazon EC2 distribuir la capacidad de la flota dentro de cada opción de compra.

También puede establecer la cantidad máxima por hora que está dispuesto a pagar por su flota y la flota de EC2 lanza instancias hasta que se alcance la cantidad máxima. Cuando se alcanza la cantidad máxima por hora que está dispuesto a pagar, la flota deja de lanzar instancias incluso si no se ha alcanzado la capacidad de destino.

La flota de EC2 intenta iniciar el número de instancias que se requieren para satisfacer la capacidad de destino que haya especificado en su solicitud. Si especifica un precio máximo total por hora, satisface la capacidad hasta que se alcanza la cantidad máxima que está dispuesto a pagar. Además, la flota puede intentar mantener la capacidad de spot de destino si las instancias de spot se interrumpen. Para obtener más información, consulte Cómo funcionan las instancias de spot.



Puede especificar un número ilimitado de tipos de instancias por flota de EC2. Esos tipos de instancias se pueden aprovisionar tanto con las opciones de compra bajo demanda como de spot. También puede seleccionar varias zonas de disponibilidad, especificar los distintos precios de spot máximos para cada instancia y elegir opciones de spot adicionales para cada flota. Amazon EC2 utiliza las opciones especificadas para aprovisionar capacidad cuando se inicia la flota.

Mientras la flota se está ejecutando, si Amazon EC2 reclama una instancia de spot debido a un incremento de los precios o a que una instancia devolvió un error, la flota de EC2 puede reemplazar las instancias por cualquiera de los tipos de instancias que se especifiquen. De ese modo, resulta

más sencillo recuperar la capacidad durante un pico de los precios de spot. Puede desarrollar una estrategia de asignación de recursos flexible y elástica para cada flota. Por ejemplo, dentro de las flotas específicas, su capacidad principal puede ser bajo demanda y complementarla con capacidad de spot más barata en caso de que esté disponible.

Si tiene instancias reservadas y especifica instancias en diferido en la flota, la flota de EC2 usará instancias reservadas. Por ejemplo, si la flota especifica una instancia a petición como `c4.large` y usted tiene instancias reservadas para `c4.large`, recibirá el precio de instancia reservada. Lo mismo se aplica si utiliza un Savings Plan.

El uso de la flota de EC2 no supone ningún cargo adicional. Únicamente se pagan las instancias EC2 que la flota inicia en su nombre.

Contenido

Limitaciones de la flota de EC2

Las limitaciones siguientes son aplicables a la flota de EC2:

- La flota de EC2 solo está disponible a través de la API de Amazon EC2, AWS CLI, SDK de AWS y AWS CloudFormation.
- Una solicitud de flota de EC2 no puede abarcar varias regiones de AWS. Es preciso crear una flota de EC2 independiente para cada región.
- Una solicitud de flota de EC2 no puede abarcar diferentes subredes de la misma zona de disponibilidad.

Instancias de rendimiento ampliable

Si inicia instancias de spot mediante un tipo de instancias de rendimiento ampliable y si piensa utilizar instancias de spot de rendimiento ampliable inmediatamente y durante un corto periodo de tiempo, sin tiempo de inactividad para acumular créditos de CPU, le recomendamos que las

lance en modo estándar para evitar pagar costos más elevados. Si inicia instancias de spot de rendimiento ampliable en modo ilimitado y amplía el uso de la CPU inmediatamente, gastará créditos sobrantes para el rendimiento ampliable. Si utiliza la instancia durante un periodo corto de tiempo, la instancia no tiene tiempo de acumular créditos de CPU para compensar los créditos sobrantes y se le cobrarán dichos créditos sobrantes al terminar la instancia.

El modo ilimitado resulta adecuado para instancias de spot de rendimiento ampliable solo si la instancia se ejecuta el tiempo suficiente para acumular créditos de CPU para el rendimiento ampliable. De lo contrario, al tener que pagar los créditos sobrantes, las instancias de spot con rendimiento ampliable serán más caras que otras instancias. Para obtener más información, consulte Cuando utilizar el modo ilimitado en lugar del modo de CPU fija.

Los créditos de lanzamiento tienen como objetivo ofrecer una experiencia de lanzamiento inicial productiva para instancias T2 proporcionando recursos de computación suficientes para configurar la instancia. No se permiten inicializaciones repetidas de instancias T2 para acceder a nuevos créditos de inicialización. Si necesita una CPU sostenida, puede ganar créditos (mediante un periodo de reposo), utilizar el modo ilimitado para las instancias de spot T2 o utilizar un tipo de instancia con CPU dedicada.

Tipos de solicitudes de flota de EC2

Existen tres tipos diferentes de solicitudes de flota de EC2:

`instant`

Si configura el tipo de solicitud como `instant`, la flota de EC2 realiza una solicitud puntual síncrona para la capacidad deseada. Como respuesta a la API, devuelve las instancias que se iniciaron, junto con los errores para aquellas instancias que no se pudieron iniciar. Para obtener más información, consulte Utilizar una flota de EC2 de tipo “instantáneo”.

`request`

Si configura el tipo de solicitud como `request`, la flota de EC2 realiza una solicitud puntual asíncrona para la capacidad deseada. A partir de allí, si la capacidad disminuye debido a interrupciones de spot, la flota no intentará reponer Instancias de spot, ni enviará solicitudes en grupos alternativos de spot si la capacidad no está disponible.

`maintain`

(Predeterminado) Si configura el tipo de solicitud como `maintain`, la flota de EC2 realiza una solicitud asíncrona para la capacidad deseada y conserva la capacidad completando automáticamente las instancias de spot interrumpidas.

Los tres tipos de solicitudes se benefician de la estrategia de asignación. Para obtener más información, consulte Estrategias de asignación de instancias de spot.

Utilizar una flota de EC2 de tipo “instantáneo”

La flota de EC2 de tipo instantáneo es una solicitud puntual síncrona que realiza un solo intento de iniciar la capacidad deseada. La respuesta de la API incluye una lista de las instancias que se iniciaron, así como los errores relacionados con aquellas instancias que no se pudieron iniciar. Utilizar una flota de EC2 de tipo instantáneo ofrece varios beneficios, que se describen en este artículo. Al final del artículo, se proporcionan configuraciones de ejemplo.

Para cargas de trabajo que requieren una API de inicio único para iniciar instancias EC2, puede utilizar la API RunInstances. Sin embargo, con RunInstances solo puede iniciar instancias bajo demanda o instancias de spot, pero no ambas en la misma solicitud. Además, cuando utiliza RunInstances para iniciar instancias de spot, su solicitud de instancia de spot se limita a un tipo de instancias y a una zona de disponibilidad. Esto se dirige a un único grupo de capacidad de spot (un conjunto de instancias que no se utilizan con el mismo tipo de instancias y zona de disponibilidad). Si el grupo de capacidad de spot no tiene suficiente capacidad de instancia de spot para su solicitud, se produce un error en la llamada a RunInstances.

En lugar de utilizar RunInstances para iniciar instancias de spot, recomendamos que utilice la API CreateFleet con el parámetro `type` establecido en `instant` a fin de obtener los siguientes beneficios:

- Iniciar instancias bajo demanda e instancias de Spot en una sola solicitud. Una flota de EC2 puede iniciar instancias bajo demanda, instancias de spot o ambas. La solicitud de Instancias de spot se atiende si hay capacidad disponible y el precio máximo por hora especificado en la solicitud es superior al precio de spot.
- Aumentar la disponibilidad de las instancias de spot. Con una flota de EC2 de tipo `instant`, puede iniciar instancias de spot de acuerdo con las prácticas recomendadas para instancias de spot con los beneficios resultantes:

- Práctica recomendada para instancias de spot: sea flexible con respecto a los tipos de instancias y las zonas de disponibilidad.

  Beneficio: al especificar varios tipos de instancias y zonas de disponibilidad, aumenta el número de grupos de capacidad de spot. Esto da al servicio de spot una mejor oportunidad de encontrar y asignar la capacidad informática de spot deseada. Una buena regla general es ser flexible con al menos 10 tipos de instancias para cada carga de trabajo y asegurarse de que todas las zonas de disponibilidad se encuentren configuradas a fin de utilizarse en la VPC.

- Práctica recomendada de spot: utilizar la estrategia de asignación price-capacity-optimized.

  Beneficio: la estrategia de asignación `price-capacity-optimized` identifica las instancias de los grupos de capacidad de spot que se encuentran con mayor disponibilidad y luego aprovisiona de manera automática las instancias de los grupos con los precios más bajos. Debido a que la capacidad de la instancia de spot proviene de grupos con capacidad óptima, esto disminuye la posibilidad de que se interrumpan las instancias de spot cuando Amazon EC2 vuelva a necesitar la capacidad.

- Obtener acceso a un conjunto más amplio de capacidades. Para cargas de trabajo que necesitan una API de solo inicialización y cuando prefiera administrar el ciclo de vida de su instancia en lugar de permitir que lo haga la flota de EC2, utilice la flota de EC2 de tipo `instant` en lugar de la API RunInstances. La flota de EC2 proporciona un conjunto más amplio de capacidades que RunInstances, como se demuestra en los siguientes ejemplos. Para todas las demás cargas de trabajo, debe utilizar Amazon EC2 Auto Scaling, ya que proporciona un conjunto de características más completo para una amplia variedad de cargas de trabajo, como aplicaciones respaldadas por ELB, cargas de trabajo en contenedores y trabajos de procesamiento de colas.

Puede utilizar una flota de EC2 de tipo instantáneo para lanzar instancias en Bloques de capacidad. Para obtener más información, consulte Tutorial: Inicialización de instancias en bloques de capacidad.

Los servicios de AWS como Amazon EC2 Auto Scaling y Amazon EMR utilizan la flota de EC2 de tipo instantáneo para iniciar instancias EC2.

Requisitos previos para la flota de EC2 de tipo instantáneo

Para obtener los requisitos previos a fin de crear una flota de EC2, consulte Requisitos previos de flota de EC2.

Funcionamiento de la flota de EC2 de tipo instantáneo

Cuando se trabaja con una flota de EC2 de tipo `instant`, la secuencia de eventos es la siguiente:

1. Establezca el tipo de solicitud CreateFleet en `instant`. Para obtener más información, consulte Crear una flota de EC2. Tenga en cuenta que después de realizar la llamada a la API, no podrá modificarla.
2. Cuando realiza la llamada a la API, la flota de EC2 realiza una solicitud puntual síncrona para la capacidad deseada.
3. La respuesta de la API enumera las instancias que se lanzaron, junto con los errores para esas instancias que no se pudieron lanzar.
4. Puede describir la flota de EC2 y ver su historial, así como también enumerar las instancias asociadas a ella.
5. Una vez que se hayan iniciado las instancias, puede eliminar la solicitud de flota. Al eliminar la solicitud de flota, también puede optar por terminar las instancias asociadas o dejarlas en ejecución.
6. Puede terminar las instancias en cualquier momento.

Ejemplos

En los siguientes ejemplos, se muestra cómo utilizar la flota de EC2 de tipo `instant` para diferentes casos de uso. Para obtener más información sobre el uso de los parámetros de la API CreateFleet de EC2, consulte CreateFleet en la Referencia de la API de Amazon EC2.

Ejemplos

- Ejemplo 1: iniciar instancias de spot con la estrategia de asignación de capacidad optimizada
- Ejemplo 2: iniciar una única instancia de spot con la estrategia de asignación de capacidad optimizada
- Ejemplo 3: iniciar instancias de spot con ponderación de instancias
- Ejemplo 4: iniciar instancias de spot en una sola zona de disponibilidad
- Ejemplo 5: iniciar instancias de spot de tipo de instancia único dentro de una sola zona de disponibilidad
- Ejemplo 6: iniciar instancias de spot solo si es posible iniciar la capacidad mínima de destino
- Ejemplo 7: iniciar instancias de spot solo si es posible iniciar la capacidad mínima de destino del mismo tipo de instancias en una sola zona de disponibilidad

- Ejemplo 8: iniciar instancias con varias plantillas de inicialización
- Ejemplo 9: iniciar instancias de spot con una base de instancias bajo demanda
- Ejemplo 10: iniciar instancias de spot mediante una estrategia de asignación de capacidad optimizada con una base de instancias bajo demanda con reservas de capacidad y la estrategia de asignación prioritaria
- Ejemplo 11: iniciar instancias de spot con una estrategia de asignación prioritaria de capacidad optimizada

Ejemplo 1: iniciar instancias de spot con la estrategia de asignación de capacidad optimizada

En el siguiente ejemplo, se especifican los parámetros que se requieren en una flota de EC2 de tipo `instant` (instantáneo): una plantilla de inicialización, la capacidad de destino, la opción de compra predeterminada y las modificaciones de la plantilla de inicialización.

- La plantilla de lanzamiento se identifica por su nombre y número de versión.
- Las 12 modificaciones de la plantilla de inicialización especifican 4 tipos de instancias diferentes y 3 subredes diferentes, cada una en una zona de disponibilidad distinta. Cada combinación de tipos de instancias y subredes define un grupo de capacidad de spot, lo que da como resultado 12 grupos de capacidad de spot.
- La capacidad de destino para la flota es de 20 instancias.
- La opción de compra predeterminada es `spot`, lo que resulta en que la flota intente iniciar 20 instancias de spot en el grupo de capacidad de spot con capacidad óptima para el número de instancias que se iniciarán.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.large",
```

```
            "SubnetId":"subnet-fae8c380"
         },
         {
            "InstanceType":"c5.large",
            "SubnetId":"subnet-e7188bab"
         },
         {
            "InstanceType":"c5.large",
            "SubnetId":"subnet-49e41922"
         },
         {
            "InstanceType":"c5d.large",
            "SubnetId":"subnet-fae8c380"
         },
         {
            "InstanceType":"c5d.large",
            "SubnetId":"subnet-e7188bab"
         },
         {
            "InstanceType":"c5d.large",
            "SubnetId":"subnet-49e41922"
         },
         {
            "InstanceType":"m5.large",
            "SubnetId":"subnet-fae8c380"
         },
         {
            "InstanceType":"m5.large",
            "SubnetId":"subnet-e7188bab"
         },
         {
            "InstanceType":"m5.large",
            "SubnetId":"subnet-49e41922"
         },
         {
            "InstanceType":"m5d.large",
            "SubnetId":"subnet-fae8c380"
         },
         {
            "InstanceType":"m5d.large",
            "SubnetId":"subnet-e7188bab"
         },
         {
            "InstanceType":"m5d.large",
```

```
                "SubnetId":"subnet-49e41922"
            }
          ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Ejemplo 2: iniciar una única instancia de spot con la estrategia de asignación de capacidad optimizada

Puede iniciar de forma óptima las instancias de spot de una en una si realiza varias llamadas a la API de la flota de EC2 de tipo `instant` con TotalTargetCapacity establecido en 1.

En el siguiente ejemplo, se especifican los parámetros que se requieren en una flota de EC2 de tipo instantáneo: una plantilla de inicialización, la capacidad de destino, la opción de compra predeterminada y las modificaciones de la plantilla de inicialización. La plantilla de lanzamiento se identifica por su nombre y número de versión. Las 12 modificaciones de las plantillas de inicialización tienen 4 tipos de instancias diferentes y 3 subredes diferentes, cada una en una zona de disponibilidad distinta. La capacidad de destino de la flota es 1 instancia, y la opción de compra predeterminada es spot, lo que da como resultado que la flota intente iniciar una instancia de spot desde uno de los 12 grupos de capacidad de spot en función de la estrategia de asignación de capacidad optimizada, a fin de iniciar una instancia de spot desde el grupo de capacidad más disponible.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
```

```
            "InstanceType":"c5.large",
            "SubnetId":"subnet-fae8c380"
         },
         {
            "InstanceType":"c5.large",
            "SubnetId":"subnet-e7188bab"
         },
         {
            "InstanceType":"c5.large",
            "SubnetId":"subnet-49e41922"
         },
         {
            "InstanceType":"c5d.large",
            "SubnetId":"subnet-fae8c380"
         },
         {
            "InstanceType":"c5d.large",
            "SubnetId":"subnet-e7188bab"
         },
         {
            "InstanceType":"c5d.large",
            "SubnetId":"subnet-49e41922"
         },
         {
            "InstanceType":"m5.large",
            "SubnetId":"subnet-fae8c380"
         },
         {
            "InstanceType":"m5.large",
            "SubnetId":"subnet-e7188bab"
         },
         {
            "InstanceType":"m5.large",
            "SubnetId":"subnet-49e41922"
         },
         {
            "InstanceType":"m5d.large",
            "SubnetId":"subnet-fae8c380"
         },
         {
            "InstanceType":"m5d.large",
            "SubnetId":"subnet-e7188bab"
         },
         {
```

```
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-49e41922"
             }
          ]
       }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 1,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Ejemplo 3: iniciar instancias de spot con ponderación de instancias

En los siguientes ejemplos se usa ponderación de instancias, que significa que el precio se determina por hora de unidad en lugar de por hora de instancia. Cada configuración de inicialización muestra un tipo de instancias y una ponderación diferentes en función de la cantidad de unidades de la carga de trabajo que se pueden ejecutar en la instancia, si se supone que una unidad de la carga de trabajo requiere 15 GB de memoria y 4 vCPU. Por ejemplo, m5.xlarge (4 vCPU y 16 GB de memoria) puede ejecutar una unidad y tiene una ponderación de 1, m5.2xlarge (8 vCPU y 32 GB de memoria) puede ejecutar dos unidades y tiene una ponderación de 2, y así sucesivamente. La capacidad total de destino se establece en 40 unidades. La opción de compra predeterminada es de spot y la estrategia de asignación es de capacidad optimizada, lo que da como resultado 40 m5.xlarge (40 dividido por 1), 20 m5.2xlarge (40 dividido por 2), 10 m5.4xlarge (40 dividido por 4), 5 m5.8xlarge (40 dividido por 8) o una combinación de los tipos de instancias con ponderaciones que se suman a la capacidad deseada según la estrategia de asignación de capacidad optimizada.

Para obtener más información, consulte Ponderación de instancias de la flota de EC2.

```
{
   "SpotOptions":{
      "AllocationStrategy":"capacity-optimized"
   },
   "LaunchTemplateConfigs":[
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
```

```
            "InstanceType":"m5.xlarge",
            "SubnetId":"subnet-fae8c380",
            "WeightedCapacity":1
         },
         {
            "InstanceType":"m5.xlarge",
            "SubnetId":"subnet-e7188bab",
            "WeightedCapacity":1
         },
         {
            "InstanceType":"m5.xlarge",
            "SubnetId":"subnet-49e41922",
            "WeightedCapacity":1
         },
         {
            "InstanceType":"m5.2xlarge",
            "SubnetId":"subnet-fae8c380",
            "WeightedCapacity":2
         },
         {
            "InstanceType":"m5.2xlarge",
            "SubnetId":"subnet-e7188bab",
            "WeightedCapacity":2
         },
         {
            "InstanceType":"m5.2xlarge",
            "SubnetId":"subnet-49e41922",
            "WeightedCapacity":2
         },
         {
            "InstanceType":"m5.4xlarge",
            "SubnetId":"subnet-fae8c380",
            "WeightedCapacity":4
         },
         {
            "InstanceType":"m5.4xlarge",
            "SubnetId":"subnet-e7188bab",
            "WeightedCapacity":4
         },
         {
            "InstanceType":"m5.4xlarge",
            "SubnetId":"subnet-49e41922",
            "WeightedCapacity":4
         },
```

```
            {
               "InstanceType":"m5.8xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":8
            },
            {
               "InstanceType":"m5.8xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":8
            },
            {
               "InstanceType":"m5.8xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":8
            }
         ]
      }
   ],
   "TargetCapacitySpecification":{
      "TotalTargetCapacity":40,
      "DefaultTargetCapacityType":"spot"
   },
   "Type":"instant"
}
```

Ejemplo 4: iniciar instancias de spot en una sola zona de disponibilidad

Puede configurar una flota para iniciar todas las instancias en una sola zona de disponibilidad al establecer las opciones de spot SingleAvailabilityZone en verdadero.

Las 12 modificaciones de plantillas de lanzamiento tienen tipos de instancias y subredes diferentes (cada una en una zona de disponibilidad independiente), pero la misma capacidad ponderada. La capacidad total de destino es de 20 instancias, la opción de compra predeterminada es de spot y la estrategia de asignación de spot es de capacidad optimizada. La flota de EC2 inicia 20 instancias de spot, todas en una sola zona de disponibilidad, desde los grupos de capacidad de spot con capacidad óptima mediante las especificaciones de inicialización.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "SingleAvailabilityZone": true
    },
    "LaunchTemplateConfigs": [
```

```
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5d.4xlarge",
```

```
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Ejemplo 5: iniciar instancias de spot de tipo de instancia único dentro de una sola zona de disponibilidad

Puede configurar una flota para iniciar todas las instancias del mismo tipo en una única zona de disponibilidad al establecer SpotOptions SingleInstanceType y SingleAvailabilityZone en verdadero.

Las 12 modificaciones de plantillas de lanzamiento tienen tipos de instancias y subredes diferentes (cada una en una zona de disponibilidad independiente), pero la misma capacidad ponderada. La capacidad total de destino es de 20 instancias, la opción de compra predeterminada es de spot y la estrategia de asignación de spot es de capacidad optimizada. La flota de EC2 inicia 20 instancias de spot del mismo tipo, todas en una sola zona de disponibilidad, desde el grupo de instancias de spot con capacidad óptima mediante las especificaciones de inicialización.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
```

```
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
```

```
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Ejemplo 6: iniciar instancias de spot solo si es posible iniciar la capacidad mínima de destino

Al establecer las opciones de spot MinTargetCapacity en la capacidad de destino mínima que desea iniciar en conjunto, puede configurar una flota para iniciar instancias solo si es posible iniciar la capacidad mínima de destino.

Las 12 modificaciones de plantillas de lanzamiento tienen tipos de instancias y subredes diferentes (cada una en una zona de disponibilidad independiente), pero la misma capacidad ponderada. La capacidad total de destino y la capacidad mínima de destino se establecen en 20 instancias, la opción de compra predeterminada es de spot y la estrategia de asignación de spot es de capacidad optimizada. La flota de EC2 inicia 20 instancias de spot desde el grupo de capacidad de spot con capacidad óptima mediante las modificaciones de plantilla de inicialización, solo si puede iniciar las 20 instancias a la vez.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "MinTargetCapacity": 20
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
```

```
        },
        "Overrides":[
           {
              "InstanceType":"c5.4xlarge",
              "SubnetId":"subnet-fae8c380"
           },
           {
              "InstanceType":"c5.4xlarge",
              "SubnetId":"subnet-e7188bab"
           },
           {
              "InstanceType":"c5.4xlarge",
              "SubnetId":"subnet-49e41922"
           },
           {
              "InstanceType":"c5d.4xlarge",
              "SubnetId":"subnet-fae8c380"
           },
           {
              "InstanceType":"c5d.4xlarge",
              "SubnetId":"subnet-e7188bab"
           },
           {
              "InstanceType":"c5d.4xlarge",
              "SubnetId":"subnet-49e41922"
           },
           {
              "InstanceType":"m5.4xlarge",
              "SubnetId":"subnet-fae8c380"
           },
           {
              "InstanceType":"m5.4xlarge",
              "SubnetId":"subnet-e7188bab"
           },
           {
              "InstanceType":"m5.4xlarge",
              "SubnetId":"subnet-49e41922"
           },
           {
              "InstanceType":"m5d.4xlarge",
              "SubnetId":"subnet-fae8c380"
           },
           {
              "InstanceType":"m5d.4xlarge",
```

```
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Ejemplo 7: iniciar instancias de spot solo si es posible iniciar la capacidad mínima de destino del mismo tipo de instancias en una sola zona de disponibilidad

Puede configurar una flota para iniciar instancias solo si es posible iniciar la capacidad mínima de destino con un único tipo de instancias en una sola zona de disponibilidad al establecer las opciones de spot MinTargetCapacity en la capacidad mínima de destino que desea iniciar en conjunto con las opciones SingleInstanceType y SingleAvailabilityZone.

Las 12 especificaciones de inicialización, que modifican la plantilla de inicialización, tienen tipos de instancias y subredes diferentes (cada una en una zona de disponibilidad independiente), pero la misma capacidad ponderada. La capacidad total de destino y la capacidad mínima de destino se establecen en 20 instancias, la opción de compra predeterminada es de spot, la estrategia de asignación de spot es de capacidad optimizada, y SingleInstanceType y SingleAvailabilityZone se establecen en true (verdadero). La flota de EC2 inicia 20 instancias de spot del mismo tipo, todas en una sola zona de disponibilidad, desde el grupo de capacidad de spot con capacidad óptima mediante las especificaciones de inicialización, solo si puede iniciar las 20 instancias a la vez.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true,
        "MinTargetCapacity": 20
    },
    "LaunchTemplateConfigs": [
      {
```

```
        "LaunchTemplateSpecification":{
           "LaunchTemplateName":"ec2-fleet-lt1",
           "Version":"$Latest"
        },
        "Overrides":[
           {
              "InstanceType":"c5.4xlarge",
              "SubnetId":"subnet-fae8c380"
           },
           {
              "InstanceType":"c5.4xlarge",
              "SubnetId":"subnet-e7188bab"
           },
           {
              "InstanceType":"c5.4xlarge",
              "SubnetId":"subnet-49e41922"
           },
           {
              "InstanceType":"c5d.4xlarge",
              "SubnetId":"subnet-fae8c380"
           },
           {
              "InstanceType":"c5d.4xlarge",
              "SubnetId":"subnet-e7188bab"
           },
           {
              "InstanceType":"c5d.4xlarge",
              "SubnetId":"subnet-49e41922"
           },
           {
              "InstanceType":"m5.4xlarge",
              "SubnetId":"subnet-fae8c380"
           },
           {
              "InstanceType":"m5.4xlarge",
              "SubnetId":"subnet-e7188bab"
           },
           {
              "InstanceType":"m5.4xlarge",
              "SubnetId":"subnet-49e41922"
           },
           {
              "InstanceType":"m5d.4xlarge",
              "SubnetId":"subnet-fae8c380"
```

```
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Ejemplo 8: iniciar instancias con varias plantillas de inicialización

Puede configurar una flota a fin de iniciar instancias con diferentes especificaciones de inicialización para diferentes tipos de instancias o grupos de tipos de instancias, al especificar varias plantillas de inicialización. En este ejemplo, queremos tener diferentes tamaños de volumen de EBS para diferentes tipos de instancias y eso se encuentra configurado en las plantillas de inicialización ec2-fleet-lt-4xl, ec2-fleet-lt-9xl y ec2-fleet-lt-18xl.

En este ejemplo, utilizamos 3 plantillas de inicialización diferentes para los 3 tipos de instancias en función de su tamaño. Las modificaciones de especificación de inicio en todas las plantillas de inicio utilizan ponderaciones de instancias según las vCPU del tipo de instancia. La capacidad total de destino es de 144 unidades, la opción de compra predeterminada es de spot y la estrategia de asignación de spot es de capacidad optimizada. La flota de EC2 puede iniciar 9 c5n.4xlarge (144 dividido por 16) con la plantilla de inicialización ec2-fleet-4xl, 4 c5n.9xlarge (144 dividido por 36) con la plantilla de inicialización ec2-fleet-9xl, 2 c5n.18xlarge (144 dividido por 72) con la plantilla de inicialización ec2-fleet-18xl o una combinación de los tipos de instancias con ponderaciones que se suman a la capacidad deseada en función de la estrategia de asignación de capacidad optimizada.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
```

```
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt-18xl",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5n.18xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":72
            },
            {
               "InstanceType":"c5n.18xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":72
            },
            {
               "InstanceType":"c5n.18xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":72
            }
         ]
      },
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt-9xl",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5n.9xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":36
            },
            {
               "InstanceType":"c5n.9xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":36
            },
            {
               "InstanceType":"c5n.9xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":36
```

```
            }
         ]
      },
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt-4xl",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5n.4xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":16
            },
            {
               "InstanceType":"c5n.4xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":16
            },
            {
               "InstanceType":"c5n.4xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":16
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 144,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Ejemplo 9: iniciar instancias de spot con una base de instancias bajo demanda

En el siguiente ejemplo, se especifica una capacidad total de destino de 20 instancias para la flota y una capacidad de destino de 5 instancias bajo demanda. La opción de compra predeterminada es de spot. La flota inicia 5 instancias bajo demanda según lo especificado, pero debe iniciar 15 instancias más para cubrir la capacidad total de destino. La opción de compra aplicada a la diferencia se calcula como TotalTargetCapacity – OnDemandTargetCapacity = DefaultTargetCapacityType, lo que da

lugar a que la flota lance 15 instancias de spot desde uno de los 12 grupos de capacidad de spot según la estrategia de asignación de capacidad optimizada.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
```

```
                "InstanceType":"m5.large",
                "SubnetId":"subnet-e7188bab"
            },
            {
                "InstanceType":"m5.large",
                "SubnetId":"subnet-49e41922"
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-fae8c380"
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-e7188bab"
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "OnDemandTargetCapacity": 5,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Ejemplo 10: iniciar instancias de spot mediante una estrategia de asignación de capacidad optimizada con una base de instancias bajo demanda con reservas de capacidad y la estrategia de asignación prioritaria

Puede configurar una flota para que utilice primero reservas de capacidad bajo demanda al iniciar instancias bajo demanda con el tipo de capacidad de destino predeterminado configurado como spot, al establecer la estrategia de uso de las Reservas de capacidad en use-capacity-reservations-first. Y si varios grupos de instancias tienen reservas de capacidad sin utilizar, se aplica la estrategia de asignación bajo demanda seleccionada. En este ejemplo, la estrategia de asignación bajo demanda es prioritaria.

En este ejemplo, hay 6 reservas de capacidad disponibles sin utilizar. Esto es inferior a la capacidad de destino bajo demanda de 10 instancias bajo demanda de la flota.

La cuenta tiene las siguientes 6 reservas de capacidad sin utilizar en 2 grupos. El número de reservas de capacidad en cada grupo lo indica AvailableInstanceCount.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 3,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 3,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

La siguiente configuración de flota solo muestra las configuraciones pertinentes para este ejemplo. La estrategia de asignación bajo demanda es prioritaria y la estrategia de uso de las Reservas de capacidad es use-capacity-reservations-first. La estrategia de asignación de spot es de capacidad optimizada. La capacidad total de destino es de 20, la capacidad de destino bajo demanda es de 10 y el tipo de capacidad de destino predeterminado es de spot.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "OnDemandOptions":{
       "CapacityReservationOptions": {
         "UsageStrategy": "use-capacity-reservations-first"
       },
       "AllocationStrategy":"prioritized"
    },
```

```
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 1.0
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 2.0
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 3.0
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 4.0
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 5.0
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 6.0
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 7.0
            },
            {
               "InstanceType":"m5.large",
```

```
                "SubnetId":"subnet-e7188bab",
                "Priority": 8.0
            },
            {
                "InstanceType":"m5.large",
                "SubnetId":"subnet-49e41922",
                "Priority": 9.0
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-fae8c380",
                "Priority": 10.0
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-e7188bab",
                "Priority": 11.0
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-49e41922",
                "Priority": 12.0
            }
        ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "OnDemandTargetCapacity": 10,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Después de crear la flota de tipo instantáneo con la configuración anterior, se inician las siguientes 20 instancias para cumplir con la capacidad de destino:

- 7 instancias c5.large bajo demanda en us-east-1a, c5.large en us-east-1a tiene más prioridad y hay 3 reservas de capacidad c5.large disponibles sin utilizar. Las reservas de capacidad se utilizan primero para iniciar 3 instancias bajo demanda y se inician 4 instancias bajo demanda adicionales de acuerdo con la estrategia de asignación bajo demanda, que es prioritaria en este ejemplo.

- 3 instancias m5.large bajo demanda en us-east-1a, m5.large en us-east-1a se prioriza en segundo lugar y hay 3 reservas de capacidad c3.large disponibles sin utilizar.
- 10 instancias de spot de uno de los 12 grupos de capacidad de spot que tiene la capacidad óptima de acuerdo con la estrategia de asignación de capacidad optimizada.

Después de lanzar la flota, puede ejecutar describe-capacity-reservations para ver cuántas reservas de capacidad sin utilizar quedan. En este ejemplo, debería ver la siguiente respuesta, que muestra que se utilizaron todas las reservas de capacidad c5.large y m5.large.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c5.large",
    "AvailableInstanceCount": 0
}
```

Ejemplo 11: iniciar instancias de spot con una estrategia de asignación prioritaria de capacidad optimizada

En el siguiente ejemplo, se especifican los parámetros que se requieren en una flota de EC2 de tipo instantáneo: una plantilla de lanzamiento, la capacidad de destino, la opción de compra predeterminada y las modificaciones de la plantilla de lanzamiento. La plantilla de lanzamiento se identifica por su nombre y número de versión. Las 12 especificaciones de inicialización que modifican la plantilla de inicialización tienen 4 tipos de instancias diferentes con una prioridad asignada y 3 subredes diferentes, cada una en una zona de disponibilidad independiente. La capacidad de destino de la flota es de 20 instancias, y la opción de compra predeterminada es de spot, lo que da como resultado que la flota intente iniciar 20 instancias de spot desde uno de los 12 grupos de capacidad de spot en función de la estrategia de asignación prioritaria de capacidad optimizada, que implementa las prioridades en la medida en que sea posible, pero primero optimiza la capacidad.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized-prioritized"
    },
```

```
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 1.0
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 1.0
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 1.0
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 2.0
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 2.0
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 2.0
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 3.0
            },
            {
               "InstanceType":"m5.large",
```

```
               "SubnetId":"subnet-e7188bab",
               "Priority": 3.0
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 3.0
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 4.0
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 4.0
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 4.0
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Estrategias de configuración de la flota de EC2

Una flota de EC2 es un grupo de instancias bajo demanda e instancias de spot. Una flota de EC2 también puede ser un grupo de instancias de bloques de capacidad.

Instancias bajo demanda e instancias de spot

La flota de EC2 intenta iniciar el número de instancias que se requieren para satisfacer la capacidad de destino que haya especificado en su solicitud de flota. La flota puede estar compuesta solo de instancias bajo demanda o solo de instancias de spot, o bien de una combinación de instancias

bajo demanda e instancias de spot. La solicitud de Instancias de spot se atiende si hay capacidad disponible y el precio máximo por hora especificado en la solicitud es superior al precio de spot. Además, la flota puede intentar mantener la capacidad de destino si las instancias de spot se interrumpen.

También puede establecer la cantidad máxima por hora que está dispuesto a pagar por su flota, y la flota de EC2 iniciará instancias hasta que se alcance la cantidad máxima. Cuando se alcanza cantidad máxima por hora que está dispuesto a pagar, la flota deja de lanzar instancias incluso si no se ha alcanzado la capacidad de destino.

Un grupo de capacidad de spot es un conjunto de instancias EC2 no utilizadas con el mismo tipo de instancia y zona de disponibilidad. Cuando crea una flota de EC2, puede incluir varias especificaciones de inicialización, que varían por tipo de instancia, zona de disponibilidad, subred y precio máximo. La flota selecciona los grupos de capacidad de spot que se usan para atender la solicitud, basándose en las especificaciones de inicialización incluidas y en su configuración. Las instancias de spot proceden de los grupos seleccionados.

Una flota de EC2 permite aprovisionar grandes cantidades de capacidad de EC2 que son razonables para la aplicación en función del número de núcleos o instancias o de la cantidad de memoria. Por ejemplo, puede especificar una flota de EC2 para iniciar una capacidad de destino de 200 instancias, de las que 130 son instancias en diferido y el resto son instancias de spot.

Instancias de bloques de capacidad

Los bloques de capacidad para ML le permiten reservar instancias de GPU para el futuro a fin de respaldar sus cargas de trabajo de machine learning (ML) de corta duración. Las instancias que se ejecutan en un bloque de capacidad se colocan automáticamente juntas dentro de Amazon EC2 UltraClusters. Para obtener más información sobre los bloques de capacidad, consulte Bloques de capacidad para ML.

Use las estrategias de configuración apropiadas para crear una flota de EC2 que satisfaga sus necesidades.

Contenido

- Reequilibrio de la capacidad
- Anulaciones de precios máximos
- Control de gastos
- Ponderación de instancias de la flota de EC2

Planificar una flota de EC2

Al planificar una flota de EC2, recomendamos que haga lo siguiente:

- Determine si desea crear una flota de EC2 que envíe una solicitud puntual síncrona o asíncrona para la capacidad de destino deseada o una que mantenga una capacidad de destino a lo largo del tiempo. Para obtener más información, consulte Tipos de solicitudes de flota de EC2.
- Determine los tipos de instancias que satisfacen los requisitos de su aplicación.
- Si ha previsto incluir instancias de spot en la flota de EC2, consulte Prácticas recomendadas para instancias de spot antes de crear la flota. Use estas prácticas recomendadas al planificar la flota, para aprovisionar las instancias al menor precio posible.
- Determine la capacidad de destino para la flota de EC2. Puede definir la capacidad de destino en instancias o en unidades personalizadas. Para obtener más información, consulte Ponderación de instancias de la flota de EC2.
- Determine qué parte de la capacidad de destino de la flota de EC2 debe ser capacidad en diferido y cuánta debe ser de spot. Puede especificar 0 para la capacidad bajo demanda, para la capacidad de spot o para ambas.
- Determine el precio por unidad, si está usando ponderación de instancias. Para calcular el precio por unidad, divida el precio por hora de instancia entre el número de unidades (o peso) que esta instancia representa. Si no utiliza la ponderación de instancias, el precio por unidad predeterminado es el precio por hora de instancia.
- Determine la cantidad máxima por hora que está dispuesto a pagar por su flota. Para obtener más información, consulte Control de gastos.
- Revise las posibles opciones para la solicitud de flota de EC2. Para obtener información acerca de los parámetros de flota, consulte create-fleet en la Referencia de los comandos de la AWS CLI. Para obtener ejemplos de configuración de flota de EC2, consulte Configuraciones de ejemplo de flota de EC2.

Estrategias de asignación de instancias de spot

La configuración de inicialización determina todos los grupos de capacidad de spot posibles (tipos de instancias y zonas de disponibilidad) desde los que la flota de EC2 puede iniciar instancias de spot. Sin embargo, al iniciar instancias, la flota de EC2 usa la estrategia de asignación que usted especifique para seleccionar los grupos específicos entre todos sus grupos posibles.

> **Note**
>
> (Solo instancias de Linux) Si configura la instancia de spot para lanzarla con la característica SEV-SNP de AMD activada, se le cobrará una tarifa de uso por hora adicional que equivale al 10 % de la tarifa horaria bajo demanda del tipo de instancia seleccionado. Si la estrategia de asignación utiliza el precio como variable, la flota de EC2 no incluye esta tarifa adicional; solo se utiliza el precio de spot.

Estrategias de asignación

Puede especificar una de las siguientes estrategias de asignación para las instancias de spot:

`price-capacity-optimized` (recomendado)

La flota de EC2 identifica los grupos con la mayor disponibilidad de capacidad para la cantidad de instancias que se van a lanzar. Esto significa que solicitaremos instancias de spot de los grupos que consideremos que tienen menos probabilidades de interrupción a corto plazo. A continuación, la flota de EC2 solicita instancias de spot de los grupos con el precio más bajo.

La estrategia de asignación de `price-capacity-optimized` es la mejor opción para la mayoría de las cargas de trabajo de spot, como las aplicaciones en contenedores sin estado, los microservicios, las aplicaciones web, los trabajos de datos y análisis y el procesamiento por lotes.

`capacity-optimized`

La flota de EC2 identifica los grupos con la mayor disponibilidad de capacidad para la cantidad de instancias que se van a lanzar. Esto significa que solicitaremos instancias de spot de los grupos que consideremos que tienen menos probabilidades de interrupción a corto plazo. Opcionalmente, puede establecer una prioridad para cada tipo de instancia de su flota utilizando `capacity-optimized-prioritized`. La flota de EC2 optimiza primero las capacidades, pero respeta las prioridades del tipo de instancia sobre la base de los mejores esfuerzos.

Con Instancias de spot, los precios cambian lentamente con el paso del tiempo en función de las tendencias a largo plazo de la oferta y la demanda, pero la capacidad fluctúa en tiempo real. La estrategia `capacity-optimized` inicia instancias de spot de forma automática en los grupos con mayor disponibilidad, analizando los datos de capacidad en tiempo real y prediciendo cuáles son los que tienen una mayor disponibilidad. Esto funciona bien para las cargas de trabajo que pueden tener un costo mayor de interrupción asociado al reinicio del trabajo, como integración continua (CI) prolongada, representación de imágenes y medios, aprendizaje profundo y computación de alto rendimiento (HPC) que pueden tener un costo mayor de interrupción asociado al reinicio del trabajo. Al ofrecer la posibilidad de experimentar menos interrupciones, la estrategia `capacity-optimized` puede reducir el costo total de la carga de trabajo.

Como alternativa, puede utilizar la estrategia de asignación `capacity-optimized-prioritized` con un parámetro de prioridad para ordenar los tipos de instancias de la prioridad más alta a la más baja. Puede establecer la misma prioridad para diferentes tipos de instancia. La flota de EC2 optimizará primero la capacidad, pero respetará las prioridades del tipo de instancia sobre la base del mejor esfuerzo (por ejemplo, si el respeto de las prioridades no afecta significativamente la capacidad de la flota de EC2 para aprovisionar una capacidad óptima). Esta es una buena opción para cargas de trabajo en las que se debe minimizar la posibilidad de interrupción y también importa la preferencia por ciertos tipos de instancias. Tenga en cuenta que cuando establece la prioridad para `capacity-optimized-prioritized`, la misma prioridad también se aplica a las instancias bajo demanda si `AllocationStrategy` bajo demanda se establece en `prioritized`.

`diversified`

Las instancias de spot se distribuyen en todos los grupos de capacidad de spot.

`lowest-price` (no recomendado)

> **Warning**
>
> No recomendamos la estrategia de asignación `lowest-price` porque presenta el mayor riesgo de interrupción para las instancias de spot.

Las instancias de spot provienen del grupo con el precio más bajo que tiene capacidad disponible. Esta es la estrategia predeterminada. Sin embargo, recomendamos que, para anular el valor predeterminado, especifique la estrategia de asignación `price-capacity-optimized`.

Si el grupo con el precio más bajo no tiene capacidad disponible, las instancias de spot provienen del siguiente grupo con el precio más bajo que tenga capacidad disponible.

Si un grupo se queda sin capacidad antes de cubrir la capacidad deseada, la flota de EC2 completará la solicitud y extraerá capacidad del siguiente grupo con el precio más bajo. Para garantizar que se logre la capacidad deseada, es posible que reciba instancias de spot de varios grupos.

Dado que esta estrategia solo tiene en cuenta el precio de la instancia y no la disponibilidad de capacidad, podría generar tasas de interrupción elevadas.

`InstancePoolsToUseCount`

El número de grupos de spot en los que asignar la capacidad de spot de destino. Solo es válido cuando la estrategia de asignación se ha establecido en `lowest-price`. La flota de EC2 selecciona los grupos de spot con el precio más bajo y asigna la capacidad de spot de destino de manera uniforme entre los grupos de spot que especifique.

Tenga en cuenta que la flota de EC2 intentará obtener instancias de spot del número de grupos que usted especifique en la medida de lo posible. Si un grupo se queda sin capacidad de spot antes de cubrir su capacidad de destino, la flota de EC2 cumplirá su solicitud y extraerá capacidad del siguiente grupo con el precio más bajo. Para garantizar que la capacidad de destino se cumpla, es posible que reciba instancias de spot de una cantidad de grupos mayor al número de grupos que usted especificó. Del mismo modo, si la mayoría de los grupos no tienen capacidad de spot, es posible que reciba su capacidad de destino total de menos grupos que el número de grupos que especificó.

Seleccionar la estrategia de asignación apropiada

Para poder optimizar su flota para su caso de uso, elija la estrategia de asignación de spot adecuada. Para la capacidad de destino de las instancias bajo demanda, la flota de EC2 siempre selecciona el tipo de instancia menos costoso en función del precio público bajo demanda, mientras que sigue la estrategia de asignación (ya sea `price-capacity-optimized`, `capacity-optimized`, `diversified` o `lowest-price`) de las instancias de spot.

Equilibrio del precio más bajo y la disponibilidad de capacidad

Para equilibrar las compensaciones entre los grupos de capacidad de spot con el precio más bajo y los grupos de capacidad de spot con la mayor disponibilidad de capacidad, le recomendamos utilizar la estrategia de asignación `price-capacity-optimized`. Esta estrategia toma decisiones

sobre a qué grupos se van a solicitar instancias de spot en función del precio de los grupos y de la disponibilidad de capacidad de las instancias de spot de esos grupos. Esto significa que solicitaremos instancias de spot a los grupos que consideremos que tienen la menor probabilidad de interrupción a corto plazo, sin dejar de tener en cuenta el precio.

Si la flota ejecuta cargas de trabajo resistentes y sin estado, como aplicaciones en contenedores, microservicios, aplicaciones web, trabajos de datos y análisis y procesamiento por lotes, utilice la estrategia de asignación `price-capacity-optimized` para obtener ahorros de costos y disponibilidad de capacidad óptimos.

Si la flota ejecuta cargas de trabajo que pueden tener un costo mayor de interrupción asociado al reinicio del trabajo, debe implementar puntos de control para que las aplicaciones puedan reiniciarse desde ese punto en caso de que se interrumpan. Al utilizar puntos de control, la estrategia de asignación `price-capacity-optimized` es una buena opción para estas cargas de trabajo, ya que asigna capacidad de los grupos con el precio más bajo y, además, ofrecen una tasa de interrupción de instancia de spot baja.

Para ver un ejemplo de configuración que utiliza la estrategia de asignación `price-capacity-optimized`, consulte Ejemplo 10: inicialización de instancias de spot en una flota price-capacity-optimized.

Cuando las cargas de trabajo tienen un alto costo de interrupción

Si lo desea, puede utilizar la estrategia `capacity-optimized` si ejecuta cargas de trabajo que utilizan tipos de instancias con precios similares o si el costo de la interrupción es tan importante que cualquier ahorro de costos es insuficiente en comparación con un aumento marginal de las interrupciones. Esta estrategia asigna capacidad de los grupos de capacidad de spot de la mayor disponibilidad que ofrecen la posibilidad de sufrir menos interrupciones, lo que puede reducir el costo total de la carga de trabajo. Para ver un ejemplo de configuración que utiliza la estrategia de asignación `capacity-optimized`, consulte Ejemplo 8: inicialización de instancias de spot en una flota de capacidad optimizada.

Cuando se debe minimizar la posibilidad de interrupción, pero la preferencia por determinados tipos de instancia es importante, puede expresar las prioridades del grupo mediante la estrategia de asignación `capacity-optimized-prioritized` y, luego, establecer el orden de los tipos de instancias que se utilizarán, de la prioridad más alta a la más baja. Para ver una configuración de ejemplo, consulte Ejemplo 9: lanzamiento de instancias de spot en una flota de capacidad optimizada con prioridades.

Tenga en cuenta que cuando establece prioridades para `capacity-optimized-prioritized`, estas también se aplican a las instancias bajo demanda si `AllocationStrategy` bajo demanda se establece en `prioritized`.

Cuando su carga de trabajo es flexible en el tiempo y la disponibilidad de la capacidad no es un factor

Si una flota es pequeña o se ejecuta durante poco tiempo, puede utilizar `price-capacity-optimized` para maximizar el ahorro de costos sin dejar de tener en cuenta la disponibilidad de capacidad.

Cuando la flota es grande o se ejecuta durante mucho tiempo

Si la flota es grande o se ejecuta durante mucho tiempo, puede mejorar su disponibilidad al distribuir las instancias de spot entre varios grupos, al usar la estrategia `diversified`. Por ejemplo, si la flota de EC2 especifica 10 grupos y una capacidad de destino de 100 instancias, la flota inicia 10 instancias de spot en cada grupo. Si el precio de spot de un grupo sobrepasa el precio máximo de ese grupo, solo el 10 % de la flota se ve afectada. El uso de esta estrategia también consigue que su flota sea menos sensible a los aumentos en el precio de spot en cualquiera de los grupos a lo largo del tiempo. Con la estrategia `diversified`, la flota de EC2 no inicia instancias de spot; en ningún grupo con un precio de spot que sea mayor o igual que el precio en diferido.

Mantener la capacidad de destino

Después de que las instancias de spot se terminen debido a un cambio en el precio de spot o en la capacidad disponible de un grupo de capacidad de spot, una flota de EC2 de tipo `maintain` inicia instancias de spot de reemplazo. La estrategia de asignación determina los grupos desde los que se inician las instancias de reemplazo, de la siguiente manera:

- Si la estrategia de asignación es `price-capacity-optimized`, la flota inicia instancias de reemplazo en los grupos que tienen la mayor disponibilidad de capacidad de instancia de spot, sin dejar de tener en cuenta el precio e identifica los grupos con el precio más bajo con alta disponibilidad de capacidad.
- Si la estrategia de asignación es `capacity-optimized`, la flota inicia instancias de reemplazo en los grupos que tienen la mayor disponibilidad de capacidad de instancia de spot.
- Si la estrategia de asignación es `diversified`, la flota distribuye las instancias de spot de reemplazo entre los grupos restantes.

Selección de tipo de instancia basada en atributos para la flota de EC2

Al crear una flota de EC2, debe especificar uno o varios tipos de instancias para configurar las instancias bajo demanda y las instancias de spot de la flota. Como alternativa a especificar de forma manual los tipos de instancia, puede especificar los atributos que debe tener una instancia y Amazon EC2 identificará todos los tipos de instancias con esos atributos. Esto se conoce como selección de tipo de instancia basada en atributos. Por ejemplo, puede especificar el número mínimo y máximo de vCPU necesarias para sus instancias, y la flota de EC2 iniciará las instancias mediante cualquier tipo de instancia disponible que cumpla esos requisitos de vCPU.

La selección de tipo de instancia basada en atributos es ideal para cargas de trabajo y marcos que pueden ser flexibles sobre los tipos de instancias que utilizan, como cuando se ejecutan contenedores o flotas web, se procesan macrodatos y se implementan herramientas de integración e implementación continuas (CI/CD).

Beneficios

La selección de tipo de instancia basada en atributos posee los siguientes beneficios:

- Uso fácil de los tipos de instancias correctos: con tantos tipos de instancias disponibles, encontrar los tipos de instancias adecuados para su carga de trabajo puede necesitar mucho tiempo. Cuando especifica atributos de instancia, los tipos de instancia tendrán automáticamente los atributos necesarios para la carga de trabajo.
- Configuración simplificada: para especificar de forma manual varios tipos de instancias para una flota de EC2, debe crear una anulación de la plantilla de inicialización independiente para cada tipo de instancia. Sin embargo, con la selección de tipo de instancia basada en atributos, para proporcionar varios tipos de instancias solo necesita especificar los atributos de instancia en la plantilla de lanzamiento o en una anulación de la plantilla de lanzamiento.
- Uso automático de nuevos tipos de instancias: cuando se especifican atributos de instancia en lugar de tipos de instancias, su flota puede utilizar tipos de instancias de nueva generación a medida que se publican, con lo que se prueba la eficiencia futura de la configuración de la flota.
- Flexibilidad del tipo de instancias: cuando se especifican atributos de instancias en lugar de tipos de instancias, la flota de EC2 puede seleccionar entre una amplia gama de tipos de instancias para iniciar instancias de spot, de forma que se siguen las prácticas recomendadas de instancias de spot de flexibilidad con respecto a los tipos de instancia.

Temas

Cómo funciona la selección de tipo de instancia basada en atributos

Para utilizar la selección de tipo de instancia basada en atributos en la configuración de la flota, debe reemplazar la lista de tipos de instancias por una lista de atributos de instancia que requieren las instancias. La flota de EC2 iniciará instancias en cualquier tipo de instancia disponible que tenga los atributos de instancia especificados.

Temas

Tipos de atributos de instancia

Hay varios atributos de instancia que puede especificar para expresar los requisitos de computación, como, por ejemplo:

- Recuento de vCPU: el número mínimo y máximo de vCPU por instancia.
- Memoria: los GiB de memoria mínimos y máximos por instancia.
- Almacenamiento local: si se usarán volúmenes de almacén de instancias o EBS para el almacenamiento local.
- Rendimiento ampliable: si se usará la familia de instancias T, incluidos los tipos T4g, T3a, T3 y T2.

Para obtener una descripción de cada atributo y los valores predeterminados, consulte InstanceRequirements en la Referencia de la API de Amazon EC2.

Dónde configurar la selección de tipo de instancia basada en atributos

Según si utiliza la consola o la AWS CLI, puede especificar los atributos de instancia para la selección de tipo de instancia basada en atributos de la siguiente manera:

En la consola, puede especificar los atributos de la instancia en el siguiente componente de configuración de la flota:

- En una plantilla de lanzamiento y, luego, hacer referencia a la plantilla de lanzamiento en la solicitud de flota

En la AWS CLI puede especificar los atributos de la instancia en uno o todos los siguientes componentes de configuración de la flota:

- En una plantilla de lanzamiento y, luego, hacer referencia a la plantilla de lanzamiento en la solicitud de flota
- En una anulación de la plantilla de inicialización

  Si desea una combinación de instancias que utilizan diferentes AMI, puede especificar atributos de instancia en varias anulaciones de plantillas de lanzamiento. Por ejemplo, distintos tipos de instancias pueden utilizar procesadores x86 y basados en Arm.

Cómo la flota de EC2 utiliza la selección de tipo de instancia basada en atributos al aprovisionar una flota

La flota de EC2 aprovisiona una flota de la siguiente manera:

- La flota de EC2 identifica los tipos de instancias que tienen los atributos especificados.
- La flota de EC2 utiliza la protección de precios para determinar qué tipos de instancias excluir.
- La flota de EC2 determina los grupos de capacidad desde los que considerará iniciar las instancias en función de las regiones o zonas de disponibilidad de AWS que tienen tipos de instancias coincidentes.
- La flota de EC2 aplica la estrategia de asignación especificada para determinar desde qué grupos de capacidad se van a iniciar las instancias.

  Tenga en cuenta que la selección de tipo de instancia basada en atributos no selecciona los grupos de capacidad desde los que se aprovisiona la flota; eso depende de las estrategias de asignación.

Si especifica una estrategia de asignación, la flota de EC2 iniciará instancias según la estrategia de asignación especificada.

- En cuanto a las instancias de spot, la selección del tipo de instancia basada en atributos admite las estrategias de asignación `price-capacity-optimized`, `capacity-optimized` y `lowest-price`. Tenga en cuenta que no recomendamos la estrategia de asignación de instancias de spot de `lowest-price` porque presenta el mayor riesgo de interrupción para las instancias de spot.
- Para las instancias bajo demanda, la selección de tipo de instancia basada en atributos admite la estrategia de asignación `lowest-price`.

- Si no hay capacidad para los tipos de instancias con los atributos de instancia especificados, no se pueden lanzar instancias y la flota devuelve un error.

Protección de precios

La protección de precios es una característica que impide que su flota de EC2 utilice tipos de instancias que consideraría demasiado caros, incluso si se ajustan a los atributos especificados. Para utilizar la protección de precios, debe establecer un umbral de precios. A continuación, cuando Amazon EC2 selecciona tipos de instancias con sus atributos, excluye los tipos de instancias con precios superiores al umbral.

La forma en que Amazon EC2 calcula el umbral de precio es la siguiente:

- En primer lugar, Amazon EC2 identifica el tipo de instancia con el precio más bajo entre los que coinciden con sus atributos.
- A continuación, Amazon EC2 toma el valor (expresado como porcentaje) que especificó para el parámetro de protección de precios y lo multiplica por el precio del tipo de instancias identificado. El resultado es el precio que se utiliza como umbral de precio.

Existen límites de precios diferentes para las instancias bajo demanda y las instancias de spot.

Cuando crea una flota con la selección del tipo de instancia basada en atributos, se habilita la protección de precios de forma predeterminada. Puede mantener los valores predeterminados o especificar los suyos.

También puede desactivar la protección de precios. Para indicar que no hay umbral de protección de precios, especifique un valor de porcentaje alto, como `999999`.

Temas

Cómo se identifica el tipo de instancia con el precio más bajo

Amazon EC2 determina el precio en el que se basará el umbral de precios mediante la identificación del tipo de instancia con el precio más bajo entre los que coinciden con los atributos especificados. Lo hace de la siguiente forma:

- En primer lugar, analiza los tipos de instancias C, M o R de la generación actual que coincidan con sus atributos. Si encuentra alguna coincidencia, identifica el tipo de instancia con el precio más bajo.
- Si no hay ninguna coincidencia, analiza los tipos de instancias de la generación actual que coincidan con sus atributos. Si encuentra alguna coincidencia, identifica el tipo de instancia con el precio más bajo.
- Si no hay ninguna coincidencia, analiza los tipos de instancias de la generación anterior que coincidan con sus atributos e identifica el tipo de instancia con el precio más bajo.

Protección de precios de las instancias bajo demanda

El umbral de protección de precios para los tipos de instancias bajo demanda se calcula como un porcentaje superior al tipo de instancia bajo demanda identificado con el precio más bajo (`OnDemandMaxPricePercentageOverLowestPrice`). Especificará el porcentaje más alto que está dispuesto a pagar. Si no especifica este parámetro, se utilizará el valor predeterminado `20` para calcular un umbral de protección de precios superior en un 20 % al precio identificado.

Por ejemplo, si el precio de la instancia bajo demanda identificada es `0.4271` y usted especificó `25`, el umbral de precios es un 25 % superior a `0.4271`. Se calcula como se indica a continuación: `0.4271 * 1.25 = 0.533875`. El precio calculado es el máximo que está dispuesto a pagar por las instancias bajo demanda y, en este ejemplo, Amazon EC2 excluirá cualquier tipo de instancia bajo demanda que cueste más de `0.533875`.

Protección de precios de instancias de spot

De manera predeterminada, Amazon EC2 aplicará automáticamente una protección óptima del precio de las instancias de spot para seleccionar de manera coherente entre una amplia gama de tipos de instancia. También puede configurar manualmente la protección de precios. Sin embargo, dejar que Amazon EC2 lo haga puede aumentar la probabilidad de que se agote la capacidad de spot.

Puede especificar manualmente la protección de precios con una de las opciones siguientes. Si configura manualmente la protección de precios, le recomendamos utilizar la primera opción.

- Un porcentaje del tipo de instancia bajo demanda identificado con el precio más bajo [`MaxSpotPriceAsPercentageOfOptimalOnDemandPrice`]

  Por ejemplo, si el precio del tipo de instancia bajo demanda identificado es `0.4271` y usted especificó `60`, el umbral de precios es un 60 % de `0.4271`. Se calcula como se indica a continuación: `0.4271 * 0.60 = 0.25626`. El precio calculado es el máximo que está dispuesto a pagar por las instancias de spot y, en este ejemplo, Amazon EC2 excluirá cualquier tipo de instancia de spot que cueste más de `0.25626`.
- Un porcentaje superior al tipo de instancia de spot identificado con el precio más bajo [`SpotMaxPricePercentageOverLowestPrice`]

  Por ejemplo, si el precio del tipo de instancia de spot identificado es `0.1808` y usted especificó `25`, el umbral de precios es un 25 % superior a `0.1808`. Se calcula como se indica a continuación: `0.1808 * 1.25 = 0.226`. El precio calculado es el máximo que está dispuesto a pagar por las instancias de spot y, en este ejemplo, Amazon EC2 excluirá cualquier tipo de instancia de spot que cueste más de `0.266`. No le recomendamos utilizar este parámetro porque los precios de spot pueden fluctuar y, por lo tanto, su umbral de protección de precios también puede fluctuar.

Especificación del umbral de protección de precios

Para especificar el límite de protección de precios

Cuando cree la flota de EC2, configure la flota para la selección del tipo de instancia basada en atributos y, a continuación, haga lo siguiente:

- Para especificar el límite de protección de precios de las instancias bajo demanda, en el archivo de configuración JSON, en la estructura `InstanceRequirements`, en

`OnDemandMaxPricePercentageOverLowestPrice`, ingrese el límite de protección de precios en forma de porcentaje.

- Para especificar el umbral de protección de precios de las instancias de spot, en el archivo de configuración JSON, en la estructura `InstanceRequirements`, especifique uno de los siguientes parámetros:
  - En `MaxSpotPriceAsPercentageOfOptimalOnDemandPrice`, ingrese el umbral de protección de precios en forma de porcentaje.
  - En `SpotMaxPricePercentageOverLowestPrice`, ingrese el umbral de protección de precios en forma de porcentaje.

Para obtener más información sobre la creación de una flota, consulte Cree una flota de EC2 con selección de tipo de instancia basada en atributos.

> **Note**
>
> Cuando crea la flota de EC2, si establece `TargetCapacityUnitType` en `vcpu` o `memory-mib`, el límite de protección de precios se aplica en función del precio por vCPU o por memoria en lugar del precio por instancia.

Consideraciones

- Puede especificar tipos de instancias o atributos de instancia en una flota de EC2, pero no ambos al mismo tiempo.

  Al utilizar la CLI, las anulaciones de la plantilla de lanzamiento anularán la plantilla de lanzamiento. Por ejemplo, si la plantilla de inicialización contiene un tipo de instancia y la anulación de la plantilla de inicialización contiene atributos de instancia, las instancias identificadas por los atributos de instancia anularán el tipo de instancia en la plantilla de inicialización.
- Al utilizar la CLI, cuando especifica atributos de instancia como anulaciones, no puede especificar ponderaciones ni prioridades al mismo tiempo.
- Puede especificar un máximo de cuatro estructuras `InstanceRequirements` en una configuración de solicitud.

Cree una flota de EC2 con selección de tipo de instancia basada en atributos

Puede configurar una flota para que utilice la selección de tipo de instancia basada en atributos mediante la AWS CLI.

Para crear una flota de EC2 con selección de tipo de instancia basada en atributos (AWS CLI)

Utilice el comando create-fleet (AWS CLI) para crear una flota de EC2. Especifique la configuración de la flota en un archivo JSON.

```
aws ec2 create-fleet \
    --region us-east-1 \
    --cli-input-json file://file_name.json
```

Archivo *file_name*.json de ejemplo

En el siguiente ejemplo, se incluyen los parámetros que configuran una flota de EC2 para utilizar la selección de tipos de instancia basada en atributos y va seguida de una explicación de texto.

```
{
 "SpotOptions": {
  "AllocationStrategy": "price-capacity-optimized"
 },
 "LaunchTemplateConfigs": [{
  "LaunchTemplateSpecification": {
   "LaunchTemplateName": "my-launch-template",
   "Version": "1"
  },
  "Overrides": [{
   "InstanceRequirements": {
    "VCpuCount": {
     "Min": 2
    },
    "MemoryMiB": {
     "Min": 4
    }
   }
  }]
 }],
 "TargetCapacitySpecification": {
  "TotalTargetCapacity": 20,
  "DefaultTargetCapacityType": "spot"
```

```
  },
  "Type": "instant"
}
```

Los atributos para la selección de tipos de instancia basada en atributos se especifican en la estructura `InstanceRequirements`. En este ejemplo, se especifican dos atributos:

- `VCpuCount`: se especifica un mínimo de 2 vCPU. Como no se especifica ningún máximo, no hay ningún límite máximo.
- `MemoryMiB`: se especifica un mínimo de 4 MiB de memoria. Como no se especifica ningún máximo, no hay ningún límite máximo.

Se identificarán los tipos de instancia que tengan 2 o más vCPU y 4 MiB o más de memoria. Sin embargo, la protección de precios y la estrategia de asignación pueden excluir algunos tipos de instancia cuando la flota de EC2 aprovisiona la flota.

Para obtener una lista y descripciones de todos los atributos posibles que se pueden especificar, consulte InstanceRequirements en la Referencia de la API de Amazon EC2.

> **Note**
>
> Cuando `InstanceRequirements` se incluye en la configuración de la flota, `InstanceType` y `WeightedCapacity` deben excluirse; no pueden determinar la configuración de la flota al mismo tiempo que los atributos de instancia.

El objeto JSON también contiene la siguiente configuración de flota:

- `"AllocationStrategy": "price-capacity-optimized"`: la estrategia de asignación de las instancias de spot de la flota.
- `"LaunchTemplateName": "my-launch-template", "Version": "1"`: la plantilla de inicialización contiene información sobre la configuración de las instancias, pero, si se especifican los tipos de instancias, se anularán con los atributos especificados en `InstanceRequirements`.
- `"TotalTargetCapacity": 20`: la capacidad de destino es de 20 instancias.
- `"DefaultTargetCapacityType": "spot"`: la capacidad predeterminada es de instancias de spot.
- `"Type": "instant"`: el tipo de solicitud para la flota es `instant`.

Ejemplos de configuraciones válidas y no válidas

Si utiliza la AWS CLI para crear una flota de EC2, debe asegurarse de que la configuración de su flota sea válida. En los siguientes ejemplos, se muestran configuraciones válidas y no válidas.

Las configuraciones no se consideran válidas cuando contienen lo siguiente:

- Una única estructura `Overrides` con `InstanceRequirements` y `InstanceType` a la vez
- Dos estructuras `Overrides`, una con `InstanceRequirements` y la otra con `InstanceType`
- Dos estructuras `InstanceRequirements` con valores de atributo superpuestos dentro de la misma `LaunchTemplateSpecification`

Configuraciones de ejemplo

- Configuración válida: plantilla de inicialización única con anulaciones
- Configuración válida: plantilla de inicialización única con varios requisitos de instancia
- Configuración válida: dos plantillas de inicialización, cada una con anulaciones
- Configuración válida: solo InstanceRequirements especificado, sin valores de atributo superpuestos
- La configuración no es válida: Overrides contiene InstanceRequirements y InstanceType
- La configuración no es válida: dos Overrides contienen InstanceRequirements y InstanceType
- La configuración no es válida: valores de atributo superpuestos

Configuración válida: plantilla de inicialización única con anulaciones

La siguiente configuración es válida. Contiene una plantilla de inicialización y otra estructura `Overrides` que contiene una estructura `InstanceRequirements`. A continuación, se presenta una explicación de texto de la configuración de ejemplo.

```
{
        "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "My-launch-template",
                "Version": "1"
                },
                "Overrides": [
                {
```

```
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 2,
                            "Max": 8
                        },
                        "MemoryMib": {
                            "Min": 0,
                            "Max": 10240
                        },
                        "MemoryGiBPerVCpu": {
                            "Max": 10000
                        },
                        "RequireHibernateSupport": true
                    }
                }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 5000,
        "DefaultTargetCapacityType": "spot",
        "TargetCapacityUnitType": "vcpu"
        }
    }
}
```

`InstanceRequirements`

Para utilizar la selección de instancias basada en atributos, debe incluir la estructura `InstanceRequirements` en la configuración de la flota y especificar los atributos deseados para las instancias de la flota.

En el ejemplo anterior, se especifican los siguientes atributos de instancia:

- `VCpuCount`: los tipos de instancia deben tener un mínimo de 2 y un máximo de 8 vCPU.
- `MemoryMiB`: los tipos de instancia deben tener un máximo de 10 240 MiB de memoria. Un mínimo de 0 indica que no hay un límite mínimo.
- `MemoryGiBPerVCpu`: los tipos de instancia deben tener un máximo de 10 000 GiB de memoria por vCPU. El parámetro `Min` es opcional. Al omitirlo, indica que no hay un límite mínimo.

`TargetCapacityUnitType`

El parámetro `TargetCapacityUnitType` especifica la unidad de la capacidad de destino. En el ejemplo, la capacidad objetivo es `5000` y el tipo de unidad de capacidad objetivo es `vcpu`, que en conjunto especifican una capacidad de destino deseada de 5000 vCPU. La flota de EC2 iniciará suficientes instancias para que el número total de vCPU de la flota sea de 5000 vCPU.

Configuración válida: plantilla de inicialización única con varios requisitos de instancia

La siguiente configuración es válida. Contiene una plantilla de inicialización y una estructura `Overrides` que contiene dos estructuras `InstanceRequirements`. Los atributos especificados en `InstanceRequirements` son válidos porque los valores no se superponen; la primera estructura `InstanceRequirements` especifica un `VCpuCount` de 0 a 2 vCPU, mientras que la segunda estructura `InstanceRequirements` especifica de 4 a 8 vCPU.

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 4,
                            "Max": 8
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
```

```
                }
              ]
            }
        ],
        "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Configuración válida: dos plantillas de inicialización, cada una con anulaciones

La siguiente configuración es válida. Contiene dos plantillas de inicialización, cada una con una estructura `Overrides` que contiene una estructura `InstanceRequirements`. Esta configuración resulta útil para el soporte de arquitectura `arm` y `x86` en la misma flota.

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "armLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "x86LaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
```

```
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
         "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Configuración válida: solo **`InstanceRequirements`** especificado, sin valores de atributo superpuestos

La siguiente configuración es válida. Contiene dos estructuras `LaunchTemplateSpecification`, cada una con una plantilla de inicialización y una estructura `Overrides` que contiene una estructura `InstanceRequirements`. Los atributos especificados en `InstanceRequirements` son válidos porque los valores no se superponen; la primera estructura `InstanceRequirements` especifica un `VCpuCount` de 0 a 2 vCPU, mientras que la segunda estructura `InstanceRequirements` especifica de 4 a 8 vCPU.

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
```

```
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            },
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyOtherLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 4,
                            "Max": 8
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
        "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

La configuración no es válida: **`Overrides`** contiene **`InstanceRequirements`** y **`InstanceType`**

La siguiente configuración no es válida. La estructura `Overrides` contiene tanto `InstanceRequirements` como `InstanceType`. En `Overrides`, puede especificar `InstanceRequirements` o `InstanceType`, pero no ambos.

```
{
```

```
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                    "InstanceType": "m5.large"
                }
              ]
            }
        ],
        "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

La configuración no es válida: dos **`Overrides`** contienen **`InstanceRequirements`** y **`InstanceType`**

La siguiente configuración no es válida. Las estructuras `Overrides` contienen tanto `InstanceRequirements` como `InstanceType`. Puede especificar `InstanceRequirements` o `InstanceType`, pero no ambos, incluso si están en diferentes estructuras `Overrides`.

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
```

```
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            },
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyOtherLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceType": "m5.large"
                }
              ]
            }
        ],
         "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

La configuración no es válida: valores de atributo superpuestos

La siguiente configuración no es válida. Cada una de las dos estructuras `InstanceRequirements` contienen `"VCpuCount": {"Min": 0, "Max": 2}`. Los valores de estos atributos se superponen, lo que dará lugar a grupos de capacidad duplicados.

```
{
        "LaunchTemplateConfigs": [
```

```
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    },
                    {
                      "InstanceRequirements": {
                          "VCpuCount": {
                              "Min": 0,
                              "Max": 2
                          },
                          "MemoryMiB": {
                              "Min": 0
                          }
                      }
                  }
                }
              ]
            }
        ],
         "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Vista previa de tipos de instancia con atributos especificados

Puede utilizar el comando de la AWS CLI get-instance-types-from-instance-requirements para obtener una vista previa de los tipos de instancias que coinciden con los atributos especificados. Esto resulta particularmente útil para determinar qué atributos se deben especificar en la configuración de

la solicitud sin iniciar ninguna instancia. Considere que el comando no tiene en cuenta la capacidad disponible.

Para obtener una vista previa de una lista de tipos de instancias al especificar atributos mediante la AWS CLI

1. (Opcional) Para generar todos los atributos posibles que se pueden especificar, utilice el comando get-instance-types-from-instance-requirements y el parámetro `--generate-cli-skeleton`. Puede dirigir de manera opcional el resultado a un archivo para guardarlo mediante `input > attributes.json`.

```
aws ec2 get-instance-types-from-instance-requirements \
    --region us-east-1 \
    --generate-cli-skeleton input > attributes.json
```

Resultado previsto

```
{
    "DryRun": true,
    "ArchitectureTypes": [
        "i386"
    ],
    "VirtualizationTypes": [
        "hvm"
    ],
    "InstanceRequirements": {
        "VCpuCount": {
            "Min": 0,
            "Max": 0
        },
        "MemoryMiB": {
            "Min": 0,
            "Max": 0
        },
        "CpuManufacturers": [
            "intel"
        ],
        "MemoryGiBPerVCpu": {
            "Min": 0.0,
            "Max": 0.0
        },
        "ExcludedInstanceTypes": [
```

```
            ""
        ],
        "InstanceGenerations": [
            "current"
        ],
        "SpotMaxPricePercentageOverLowestPrice": 0,
        "OnDemandMaxPricePercentageOverLowestPrice": 0,
        "BareMetal": "included",
        "BurstablePerformance": "included",
        "RequireHibernateSupport": true,
        "NetworkInterfaceCount": {
            "Min": 0,
            "Max": 0
        },
        "LocalStorage": "included",
        "LocalStorageTypes": [
            "hdd"
        ],
        "TotalLocalStorageGB": {
            "Min": 0.0,
            "Max": 0.0
        },
        "BaselineEbsBandwidthMbps": {
            "Min": 0,
            "Max": 0
        },
        "AcceleratorTypes": [
            "gpu"
        ],
        "AcceleratorCount": {
            "Min": 0,
            "Max": 0
        },
        "AcceleratorManufacturers": [
            "nvidia"
        ],
        "AcceleratorNames": [
            "a100"
        ],
        "AcceleratorTotalMemoryMiB": {
            "Min": 0,
            "Max": 0
        },
        "NetworkBandwidthGbps": {
```

```
            "Min": 0.0,
            "Max": 0.0
        },
        "AllowedInstanceTypes": [
            ""
        ]
    },
    "MaxResults": 0,
    "NextToken": ""
}
```

2. Cree un archivo de configuración JSON con el resultado del paso anterior y configúrelo de la siguiente manera:

> **Note**
>
> Debe proporcionar valores para `ArchitectureTypes`, `VirtualizationTypes`, `VCpuCount` y `MemoryMiB`. Puede omitir los demás atributos; cuando se omiten, se utilizan los valores predeterminados.
> Para obtener una descripción de cada atributo y sus valores predeterminados, consulte get-instance-types-from-instance-requirements en la Referencia de la línea de comandos de Amazon EC2.

   a. En `ArchitectureTypes`, especifique uno o varios tipos de arquitectura de procesador.
   b. En `VirtualizationTypes`, especifique uno o varios tipos de virtualización.
   c. En `VCpuCount`, especifique el número mínimo y máximo de vCPU. Para no especificar un límite mínimo, en `Min`, especifique `0`. Para no especificar un límite máximo, omita el parámetro `Max`.
   d. En `MemoryMiB`, especifique la cantidad mínima y máxima de memoria en MiB. Para no especificar un límite mínimo, en `Min`, especifique `0`. Para no especificar un límite máximo, omita el parámetro `Max`.
   e. De manera opcional, puede especificar uno o varios de los otros atributos para restringir aún más la lista de tipos de instancias que se devuelven.

3. Para obtener una vista previa de los tipos de instancias que tienen los atributos especificados en el archivo JSON, utilice el comando get-instance-types-from-instance-requirements y especifique el nombre y la ruta de acceso al archivo JSON mediante el parámetro `--cli-input-json`. De manera opcional, puede dar formato al resultado para que aparezca en formato de tabla.

```
aws ec2 get-instance-types-from-instance-requirements \
    --cli-input-json file://attributes.json \
    --output table
```

Archivo de ejemplo *attributes.json*

En este ejemplo, los atributos requeridos se incluyen en el archivo JSON. Ellos son `ArchitectureTypes`, `VirtualizationTypes`, `VCpuCount` y `MemoryMiB`. Además, el atributo opcional `InstanceGenerations` también se incluye. Tenga en cuenta que en `MemoryMiB`, el valor `Max` puede omitirse para indicar que no hay un límite.

```
{

    "ArchitectureTypes": [
        "x86_64"
    ],
    "VirtualizationTypes": [
        "hvm"
    ],
    "InstanceRequirements": {
        "VCpuCount": {
            "Min": 4,
            "Max": 6
        },
        "MemoryMiB": {
            "Min": 2048
        },
        "InstanceGenerations": [
            "current"
        ]
    }
}
```

Ejemplo de resultado

```
-----------------------------------------
|GetInstanceTypesFromInstanceRequirements|
+---------------------------------------+
||             InstanceTypes             ||
|+-------------------------------------+|
```

```
||             InstanceType             ||
|+-------------------------------------+|
||  c4.xlarge                          ||
||  c5.xlarge                          ||
||  c5a.xlarge                         ||
||  c5ad.xlarge                        ||
||  c5d.xlarge                         ||
||  c5n.xlarge                         ||
||  d2.xlarge                          ||
...
```

4. Después de identificar los tipos de instancia que se ajusten a sus necesidades, anote los atributos de instancia utilizados para poder utilizarlos al configurar su solicitud de flota.

Configurar flota de EC2 para copia de seguridad en diferido

Si tiene necesidades de escalado urgentes e imprevisibles (por ejemplo, en un sitio web de noticias que es preciso escalar durante un evento importante o al iniciar un juego) recomendamos especificar tipos de instancias alternativos para las de tipo instancias bajo demanda, por si no existe suficiente capacidad disponible de la opción preferida. Por ejemplo, puede que usted prefiera instancias bajo demanda `c5.2xlarge`, pero en el caso de que no haya capacidad suficiente, estaría dispuesto a utilizar algunas instancias `c4.2xlarge` durante los picos de carga. En esta situación, la flota de EC2 intentará cubrir toda la capacidad de destino con instancias `c5.2xlarge`, pero si esta no es suficiente, iniciará automáticamente instancias `c4.2xlarge` para cubrir la capacidad de destino.

Temas

- Priorizar tipos de instancias para la capacidad bajo demanda
- Utilizar reservas de capacidad para instancias bajo demanda

Priorizar tipos de instancias para la capacidad bajo demanda

Cuando la flota de EC2 intenta cubrir la capacidad bajo demanda, inicia primero de forma predeterminada el tipo de instancia con el precio más bajo. Si `AllocationStrategy` se establece en `prioritized`, la flota de EC2 aplica la prioridad para determinar qué tipo de instancia debe utilizar primero para cubrir la capacidad en diferido. La prioridad se asigna a la invalidación de la plantilla de lanzamiento y la prioridad más alta se lanza primero.

Ejemplo: priorizar tipos de instancias

En este ejemplo, se configuran tres invalidaciones de plantilla de inicialización, cada una de ellas con un tipo de instancia distinto.

El precio bajo demanda de los tipos de instancias varía. Los siguientes son los tipos de instancias que se utilizan en este ejemplo, presentados por orden de precio, comenzando por el tipo de instancia menos caro:

- `m4.large`: menos caro
- `m5.large`
- `m5a.large`

Si no se aplica la prioridad para determinar el orden, la flota cubrirá la capacidad bajo demanda comenzando por el tipo de instancia menos caro.

No obstante, supongamos que tiene instancias reservadas `m5.large` sin usar que desea utilizar primero. Puede establecer la prioridad de la invalidación de la plantilla de lanzamiento, de forma que se utilicen los tipos de instancias conforme al orden de prioridad, de la siguiente manera:

- `m5.large`: prioridad 1
- `m4.large`: prioridad 2
- `m5a.large`: prioridad 3

Utilizar reservas de capacidad para instancias bajo demanda

Con las reservas de capacidad bajo demanda, puede reservar capacidad informática para sus instancias bajo demanda en una zona de disponibilidad específica para cualquier duración. Puede configurar una flota de EC2 para que utilice primero las reservas de capacidad al iniciar instancias bajo demanda.

Las reservas de capacidad se establecen en `open` o `targeted`. La flota de EC2 puede iniciar instancias bajo demanda en las reservas de capacidad `open` o `targeted` de la siguiente manera:

- Si una reserva de capacidad es `open`, las instancias bajo demanda que tengan atributos coincidentes se ejecutarán de forma automática en la capacidad reservada.
- Si la reserva de capacidad es `targeted`, las instancias bajo demanda deben dirigirse específicamente a ella para ejecutarse en la capacidad reservada. Esto es útil para utilizar reservas de capacidad específicas o a fin de controlar cuándo se deben utilizar reservas de capacidad específicas.

Si utiliza reservas de capacidad `targeted` en su flota de EC2, debe haber suficientes reservas de capacidad para cumplir con la capacidad de destino bajo demanda; de lo contrario, falla la inicialización. Para evitar un error de inicialización, agregue las reservas de capacidad `targeted` a un grupo de recursos y, a continuación, establezca el grupo de recursos como destino. El grupo de recursos no necesita tener suficientes reservas de capacidad. Si se queda sin reservas de capacidad antes de que se cumpla la capacidad de destino bajo demanda, la flota puede iniciar la capacidad de destino restante a la capacidad bajo demanda normal.

Para utilizar las reservas de capacidad con EC2 Fleet

1. Establezca el tipo de flota en `instant`. No puede utilizar reservas de capacidad para flotas de otros tipos.
2. Establezca la estrategia de uso para las reservas de capacidad en `use-capacity-reservations-first`.
3. En la plantilla de inicialización, en Reserva de capacidad, elija Abrir o Destino por grupo. Si elige Destino por grupo, especifique el ID del grupo de recursos de las reservas de capacidad.

Cuando la flota intenta satisfacer la capacidad bajo demanda, si encuentra que varios grupos de instancias tienen reservas de capacidad coincidentes sin utilizar, determina los grupos en los que se iniciarán las instancias bajo demanda en función de la estrategia de asignación bajo demanda (`lowest-price` o `prioritized`).

Para obtener ejemplos de cómo configurar una flota para que utilice reservas de capacidad a fin de satisfacer la capacidad bajo demanda, consulte Configuraciones de ejemplo de flota de EC2, específicamente, los ejemplos 5, 6 y 7.

Para obtener información sobre cómo configurar las reservas de capacidad, consulte On-Demand Capacity Reservations y las Preguntas frecuentes sobre reservas de capacidad bajo demanda.

Reequilibrio de la capacidad

Puede configurar la flota de EC2 para iniciar una instancia de spot de reemplazo cuando Amazon EC2 emita una recomendación de reequilibrio para notificarle que una instancia de spot tiene un riesgo elevado de interrupción. El reequilibrio de la capacidad lo ayuda a mantener la disponibilidad de la carga de trabajo al aumentar de manera proactiva su flota con una nueva instancia de spot antes de que una instancia en ejecución sea interrumpida por Amazon EC2. Para obtener más información, consulte Recomendación de reequilibrio de instancias de EC2.

Para configurar una flota de EC2 para iniciar una instancia de spot de reemplazo, utilice el comando create-fleet (AWS CLI) y los parámetros relevantes de la estructura `MaintenanceStrategies`. Para obtener más información, consulte el ejemplo de configuración de inicio.

Limitaciones

- El reequilibrio de capacidad solo está disponible para flotas de tipo `maintain`.
- Mientras la flota se encuentra en ejecución, no puede modificar la configuración de reequilibrio de capacidad. Para cambiar el ajuste de reequilibrio de capacidad, debe eliminar la flota y crear una nueva.

Opciones de configuración

La `ReplacementStrategy` para la flota de EC2 admite los dos valores siguientes:

`launch-before-terminate`

Amazon EC2 termina las instancias de spot que reciben una notificación de reequilibrio después de que se inician nuevas instancias de spot de reemplazo. Cuando especifica `launch-before-terminate`, también debe especificar un valor para `termination-delay`. Después de que se inician las nuevas instancias de reemplazo, Amazon EC2 espera la duración de `termination-delay` y, luego, termina las instancias antiguas. En `termination-delay`, el mínimo es de 120 segundos (2 minutos) y el máximo es de 7200 segundos (2 horas).

Le recomendamos que utilice `launch-before-terminate` solo si puede predecir cuánto tiempo tardarán en completarse los procedimientos de cierre de instancias. Esto garantizará que las instancias anteriores terminen solo después de que se hayan completado los procedimientos de cierre. Tenga en cuenta que Amazon EC2 puede interrumpir las instancias antiguas con una advertencia de dos minutos antes del `termination-delay`.

Recomendamos no utilizar la estrategia de asignación `lowest-price` en combinación con `launch-before-terminate` para evitar tener instancias de spot de reemplazo que también tengan un riesgo elevado de interrupción.

`launch`

Amazon EC2 inicia instancias de spot de reemplazo cuando se emite una notificación de reequilibrio para las instancias de spot existentes. Amazon EC2 no termina las instancias que reciben una notificación de reequilibrio. Puede terminar las instancias anteriores o puede dejarlas en ejecución. Se cobrará por todas las instancias mientras se ejecutan.

Consideraciones

Si configura una flota de EC2 para reequilibrio de la capacidad, tenga en cuenta lo siguiente:

Proporcione tantos grupos de capacidades de spot en la solicitud como sea posible.

Configure su flota de EC2 para utilizar varios tipos de instancia y zonas de disponibilidad. Esto proporciona la flexibilidad para iniciar instancias de spot en varios grupos de capacidad de spot. Para obtener más información, consulte Sea flexible con respecto a los tipos de instancia y las zonas de disponibilidad.

Evite un riesgo elevado de interrupción de instancias de spot de reemplazo

Las instancias de spot de reemplazo pueden correr un riesgo elevado de interrupción si utiliza la estrategia de asignación `lowest-price`. Esto se debe a que Amazon EC2 siempre iniciará instancias en el grupo de menor precio que tiene capacidad disponible en ese momento, incluso si es probable que las instancias de spot de reemplazo se interrumpan poco después de iniciarse. Para evitar un riesgo elevado de interrupción, recomendamos que no utilice la estrategia de asignación `lowest-price`. En su lugar, recomendamos la estrategia de asignación `capacity-optimized` o `capacity-optimized-prioritized`. Estas estrategias garantizan que las instancias de spot de reemplazo se inicien en los grupos de capacidad de spot más óptimos; por lo tanto, es menos probable que se interrumpan en un futuro cercano. Para obtener más información, consulte Utilice la estrategia de asignación optimizada para capacidad y precio.

Amazon EC2 solo iniciará una nueva instancia si la disponibilidad es la misma o superior

Uno de los objetivos del reequilibrio de la capacidad es mejorar la disponibilidad de una instancia de spot. Si una instancia de spot existente recibe una recomendación de reequilibrio, Amazon EC2 solo iniciará una nueva instancia si esta ofrece la misma disponibilidad o una mejor que la instancia existente. Si el riesgo de interrupción de una nueva instancia es peor que el de la instancia existente, Amazon EC2 no iniciará ninguna instancia nueva. Sin embargo, Amazon EC2 seguirá evaluando los grupos de capacidad de spot e iniciará una nueva instancia si la disponibilidad mejora.

Existe la posibilidad de que la instancia existente se interrumpa sin que Amazon EC2 lance una nueva instancia de forma proactiva. Cuando esto ocurre, Amazon EC2 intentará iniciar una nueva instancia, independientemente de si la nueva instancia tiene un alto riesgo de interrupción.

El reequilibrio de la capacidad no aumenta la tasa de interrupciones de las instancias de spot

Cuando habilita el reequilibrio de capacidad, no aumenta la tasa de interrupciones de las instancias de spot (el número de instancias de spot que se reclaman cuando Amazon EC2

necesita recuperar la capacidad). Sin embargo, si el reequilibrio de capacidad detecta que una instancia está en riesgo de interrupción, Amazon EC2 intentará iniciar inmediatamente una nueva instancia. El resultado es que se pueden reemplazar más instancias en lugar de esperar a que Amazon EC2 lance una nueva después de que se interrumpa la instancia en riesgo.

Si bien es posible que se reemplacen más instancias con el reequilibrio de capacidad habilitado, se beneficia de ser proactivo en lugar de reactivo al disponer de más tiempo para tomar medidas antes de que se interrumpan las instancias. Con un aviso de interrupción de instancias de spot, normalmente solo dispone de dos minutos para apagar correctamente la instancia. Con el reequilibrio de capacidad que inicia una nueva instancia por adelantado, le da a los procesos existentes una mejor oportunidad de completarse en la instancia en riesgo, puede iniciar los procedimientos de apagado de la instancia y evitar que se programen nuevos trabajos en la instancia en riesgo. También puede empezar a preparar la instancia recién iniciada para que se haga cargo de la aplicación. Con el reemplazo proactivo del reequilibrio de capacidad, se beneficia de una continuidad estable.

Como ejemplo teórico para demostrar los riesgos y beneficios del uso del reequilibrio de capacidad, considere el siguiente escenario:

- 14:00 h: se recibe una recomendación de reequilibrio para la instancia A y Amazon EC2 comienza inmediatamente a intentar iniciar una instancia B de reemplazo, lo que le da tiempo para iniciar los procedimientos de apagado.*
- 14:30 h: se recibe una recomendación de reequilibrio para la instancia B, sustituida por la instancia C, lo que le da tiempo para iniciar los procedimientos de apagado.*
- 14:32 h: si el reequilibrio de capacidad no estuviera habilitado y si se hubiera recibido un aviso de interrupción de la instancia de spot a las 14:32 para la instancia A, solo habría tenido hasta dos minutos para actuar, pero la instancia A habría estado funcionando hasta ese momento.

* Si se especifica `launch-before-terminate`, Amazon EC2 terminará la instancia en riesgo después de que se conecte la instancia de reemplazo.

Amazon EC2 puede iniciar nuevas instancias de spot de reemplazo hasta que la capacidad utilizada sea el doble de la capacidad de destino

Cuando una flota de EC2 se configura para reequilibrio de la capacidad, la flota intenta iniciar una nueva instancia de spot de reemplazo para cada instancia de spot que recibe una recomendación de reequilibrio. Después de que una instancia de spot reciba una recomendación de reequilibrio, ya no se cuenta como parte de la capacidad cumplida. Según la estrategia de reemplazo, Amazon EC2 termina la instancia después de un retraso de terminación preconfigurado o la deja en ejecución. Esto le da la oportunidad de realizar acciones de reequilibrio en la instancia.

Si su flota alcanza el doble de su capacidad de destino, deja de iniciar nuevas instancias de reemplazo, incluso si las propias instancias de reemplazo reciben una recomendación de reequilibrio.

Por ejemplo, puede crear una flota de EC2 con una capacidad de destino de 100 instancias de spot. Todas las instancias de spot reciben una recomendación de reequilibrio, que provoca que Amazon EC2 lance 100 instancias de spot de reemplazo. Esto eleva el número de instancias de spot utilizadas a 200, lo que es el doble de la capacidad de destino. Algunas de las instancias de reemplazo reciben una recomendación de reequilibrio, pero no se inician más instancias de reemplazo porque la flota no puede exceder el doble de su capacidad objetivo.

Tenga en cuenta que se le cobrarán todas las instancias mientras se ejecutan.

Recomendamos que configure la flota de EC2 para terminar las instancias de spot que reciben una recomendación de reequilibrio

Si configura su flota de EC2 para reequilibrio de la capacidad, recomendamos que elija `launch-before-terminate` con un retraso de terminación adecuado solo si puede predecir cuánto tardarán los procedimientos de cierre de la instancia en completarse. Esto garantizará que las instancias anteriores terminen solo después de que se hayan completado los procedimientos de cierre.

Si elige terminar las instancias recomendadas para reequilibrio, le recomendamos que monitoree la señal de recomendación de reequilibrio recibida por las instancias de spot de la flota. Mediante la supervisión de la señal, puede realizar rápidamente acciones de reequilibrio en las instancias afectadas antes de que Amazon EC2 las interrumpa y luego puede finalizarlas manualmente. Si no termina las instancias, continuará pagándolas mientras se ejecuten. Amazon EC2 no termina automáticamente las instancias que reciben una recomendación de reequilibrio.

Puede configurar notificaciones mediante Amazon EventBridge o metadatos de instancia. Para obtener más información, consulte Monitorear las señales de recomendación de reequilibrio.

La flota de EC2 no cuenta las instancias que reciben una recomendación de reequilibrio al calcular la capacidad utilizada durante el escalado ascendente o descendente

Si la flota de EC2 está configurada para reequilibrio de la capacidad y cambia la capacidad de destino, ya sea para escalado ascendente o descendente, la flota no cuenta las instancias marcadas para el reequilibrio como parte de la capacidad utilizada, de la siguiente manera:

- Reducción horizontal: si reduce la capacidad de destino deseada, Amazon EC2 termina las instancias que no están marcadas para reequilibrar hasta que se alcance la capacidad

deseada. Las instancias marcadas para el reequilibrio no se cuentan para la capacidad utilizada.

Por ejemplo, puede crear una flota de EC2 con una capacidad de destino de 100 instancias de spot. 10 instancias reciben una recomendación de reequilibrio, por lo que Amazon EC2 inicia 10 nuevas instancias de reemplazo, lo que da como resultado una capacidad utilizada de 110 instancias. A continuación, se reduce la capacidad de destino a 50 (reducción horizontal), pero la capacidad utilizada es en realidad de 60 instancias porque Amazon EC2 no termina las 10 instancias marcadas para el reequilibrio. Debe terminar manualmente estas instancias o puede dejarlas en ejecución.

- Escalado horizontal: si aumenta la capacidad de destino deseada, Amazon EC2 lanza nuevas instancias hasta que se alcance la capacidad deseada. Las instancias marcadas para el reequilibrio no se cuentan para la capacidad utilizada.

  Por ejemplo, puede crear una flota de EC2 con una capacidad de destino de 100 instancias de spot. Diez instancias reciben una recomendación de reequilibrio, por lo que la flota inicia diez nuevas instancias de reemplazo, lo que da como resultado una capacidad utilizada de 110 instancias. A continuación, aumenta la capacidad de destino a 200 (escalado ascendente), pero la capacidad utilizada es en realidad 210 instancias porque las 10 instancias marcadas para el reequilibrio no son contadas por la flota como parte de la capacidad de destino. Debe terminar manualmente estas instancias o puede dejarlas en ejecución.

Anulaciones de precios máximos

Cada flota de EC2 puede incluir un precio máximo global o usar el predeterminado (el precio en diferido). La flota usa este precio como el máximo predeterminado para cada una de sus especificaciones de inicialización.

Si lo desea, puede especificar un precio máximo en una o más especificaciones de lanzamiento. Este precio es específico de la especificación de lanzamiento. Si una especificación de inicialización incluye un precio específico, la flota de EC2 usa este precio máximo para invalidar el global. Cualquier otra especificación de lanzamiento que no incluya un precio máximo específico seguirá usando el precio máximo global.

Control de gastos

La flota de EC2 deja de iniciar instancias cuando se cumple uno de los siguientes parámetros: la `TotalTargetCapacity` o el `MaxTotalPrice` (la cantidad máxima que está dispuesto a pagar).

Para controlar la cantidad que paga por hora por su flota, puede especificar el `MaxTotalPrice`. Cuando se alcanza el precio máximo total, la flota de EC2 deja de iniciar instancias incluso si no se ha alcanzado la capacidad de destino.

En los siguientes ejemplos, se muestran dos situaciones diferentes. En el primero, la flota de EC2 deja de iniciar instancias cuando se alcanza la capacidad de destino. En el segundo, la flota de EC2 deja de iniciar instancias cuando se alcanza la cantidad máxima que está dispuesto a pagar (`MaxTotalPrice`).

Ejemplo: dejar de lanzar instancias cuando se alcanza la capacidad de destino

Dada una solicitud de Instancias bajo demanda`m4.large`, donde:

- Precio bajo demanda: 0,10 USD por hora
- `OnDemandTargetCapacity`: 10
- `MaxTotalPrice`: 1,50 USD

La flota de EC2 inicia 10 instancias en diferido porque el total de 1,00 USD (10 instancias x 0,10 USD) no supera el `MaxTotalPrice` de 1,50 USD para instancias en diferido.

Ejemplo: dejar de lanzar instancias cuando se alcanza el precio máximo total

Dada una solicitud de Instancias bajo demanda`m4.large`, donde:

- Precio bajo demanda: 0,10 USD por hora
- `OnDemandTargetCapacity`: 10
- `MaxTotalPrice`: 0,80 USD

Si la flota de EC2 inicia la capacidad de destino en diferido (10 instancias en diferido), el coste total por hora sería de 1,00 USD. Esto es más que la cantidad especificada (0,80 USD) como `MaxTotalPrice` para instancias bajo demanda. Para evitar gastar más de lo que está dispuesto a pagar, la flota de EC2 inicia solo 8 instancias en diferido (por debajo de la capacidad de destino en diferido) porque la inicialización de más superaría el `MaxTotalPrice` para instancias en diferido.

Ponderación de instancias de la flota de EC2

Al crear una flota de EC2, puede definir las unidades de capacidad con que cada tipo de instancia contribuye al rendimiento de su aplicación. Luego puede ajustar el precio máximo para cada especificación de inicialización con la ponderación de instancias.

De forma predeterminada, el precio se especifica por hora de instancia. Cuando se utiliza la característica de ponderación de instancias, el precio se especifica por hora de unidad. Puede calcular el precio por hora de unidad mediante la división del precio de un tipo de instancia por el número de unidades que representa. La flota de EC2 calcula el número de instancias que debe iniciar mediante la división de la capacidad de destino por la ponderación de instancias. Si el resultado no es un entero, la flota lo redondea al siguiente entero, de manera que el tamaño de la flota no esté por debajo de su capacidad de destino. La flota puede seleccionar cualquier grupo que indique en la especificación de inicialización, incluso si la capacidad de las instancias iniciadas sobrepasa la capacidad de destino solicitada.

En la siguiente tabla se incluyen ejemplos de cálculos para determinar el precio por unidad para una flota de EC2 con una capacidad de destino de 10.

Tipo de instancia	Ponderación de instancia	Capacidad de destino	Número de instancias iniciadas	Precio por hora de instancia	Precio por hora de unidad
`r3.xlarge`	2	10	5 (10 dividido por 2)	0,05 USD	0,025 USD (0,05 dividido por 2)
`r3.8xlarge`	8	10	2 (10 dividido por 8, con el resultado redondeado hacia arriba)	0,10 USD	0,0125 USD (0,10 dividido por 8)

Use la ponderación de instancias de la flota de EC2 de la siguiente manera para aprovisionar la capacidad de destino que desea en los grupos con el precio más bajo por unidad en el momento de su tramitación:

1. Establezca la capacidad de destino de la flota de EC2 en instancias (opción predeterminada) o en las unidades de su elección, como CPU virtuales, memoria, almacenamiento o rendimiento.
2. Establezca el precio por unidad.
3. Para cada especificación de inicialización, indique la ponderación, que es el número de unidades con el que el tipo de instancia representa la capacidad de destino.

Ejemplo de ponderación de instancias

Considere una solicitud de flota de EC2 con la siguiente configuración:

- Una capacidad de destino de 24
- Una especificación de inicialización con un tipo de instancia `r3.2xlarge` y una ponderación de 6
- Una especificación de inicialización con un tipo de instancia `c3.xlarge` y una ponderación de 5

La ponderación representa el número de unidades con el que el tipo de instancia representa la capacidad de destino. Si la primera especificación de inicialización proporciona el precio por unidad más bajo (precio para `r3.2xlarge` por hora de instancia dividido entre 6), la flota de EC2 debería iniciar cuatro de estas instancias (24 dividido entre 6).

Si la segunda especificación de inicialización proporciona el precio por unidad más bajo (precio para `c3.xlarge` por hora de instancia dividido entre 5), la flota de EC2 debería iniciar cinco de estas instancias (24 dividido entre 5, con el resultado redondeado hacia arriba).

Ponderación de instancias y estrategia de asignación

Considere una solicitud de flota de EC2 con la siguiente configuración:

- Una capacidad de destino de 30 instancias de spot
- Una especificación de lanzamiento con un tipo de instancia `c3.2xlarge` y una ponderación de 8
- Una especificación de lanzamiento con un tipo de instancia `m3.xlarge` y una ponderación de 8
- Una especificación de lanzamiento con un tipo de instancia `r3.xlarge` y una ponderación de 8

La flota de EC2 debería iniciar cuatro instancias (30 dividido por 8, con el resultado redondeado hacia arriba). Con la estrategia `diversified`, la flota inicia una instancia en cada uno de los tres grupos y la cuarta instancia en cualquiera de los tres grupos que proporcione el menor precio por unidad.

Trabajar con Flotas de EC2

Para usar una flota de EC2, cree una solicitud que incluya la capacidad de destino total, la capacidad en diferido, la capacidad de spot, una o varias especificaciones de inicialización para las instancias y el precio máximo que está dispuesto a pagar. La solicitud de flota deberá incluir una plantilla de inicialización que defina la información que la flota requiere para iniciar una instancia, como una AMI, un tipo de instancia, una subred o una zona de disponibilidad y uno o varios grupos de seguridad. Puede especificar anulaciones de las especificaciones de inicialización para el tipo de instancia, la subred, la zona de disponibilidad y el precio máximo que está dispuesto a pagar, así como asignar una capacidad ponderada a cada anulación de las especificaciones de inicialización.

La flota de EC2 inicia las instancias en diferido cuando hay capacidad disponible e inicia las instancias de spot cuando el precio máximo que ha indicado es superior al precio de spot y hay capacidad disponible.

Si la flota incluye Instancias de spot, Amazon EC2 puede intentar mantener la capacidad de destino de la flota cuando los precios de spot cambien.

Una solicitud de flota de EC2 de tipo `maintain` o `request` permanece activa hasta que caduca o hasta que usted la elimina. Al eliminar una flota de tipo `maintain` o `request`, puede especificar si la eliminación terminará las instancias contenidas en esa flota. De lo contrario, las instancias bajo demanda se ejecutarán hasta que usted las termine, y las instancias de spot se ejecutarán hasta que se interrumpan o usted las termine.

Contenido

Estados de una solicitud de flota de EC2

Una solicitud de flota de EC2 puede tener uno de los siguientes estados:

`submitted`

La solicitud de flota de EC2 está en evaluación y Amazon EC2 se prepara para lanzar el número de instancias de destino. La solicitud puede incluir instancias bajo demanda, instancias de spot o ambos. Si una solicitud excede los límites de la flota, se elimina inmediatamente.

`active`

La solicitud de flota de EC2 se ha validado y Amazon EC2 está intentando mantener el número de destino de instancias de ejecución. La solicitud permanece en este estado hasta que se modifica o se elimina.

`modifying`

La solicitud de flota de EC2 se está modificando. La solicitud permanece en este estado hasta que la modificación se procesa completamente o se elimina la solicitud. Sólo un tipo de flota `maintain` se puede modificar. Este estado no se aplica a otros tipos de solicitud.

`deleted_running`

La solicitud de flota de EC2 se ha eliminado y no lanza instancias adicionales. Las instancias existentes de la flota continúan en ejecución hasta que se interrumpen o se terminan manualmente. La solicitud permanece en este estado hasta que se interrumpan o terminen todas las instancias. Solo una flota de EC2 de tipo `maintain` o `request` puede tener instancias de ejecución después de que la solicitud de flota de EC2 sea eliminada. No se admite una flota `instant` eliminada con instancias en ejecución. Este estado no se aplica a `instant` las flotas.

`deleted_terminating`

La solicitud de flota de EC2 se ha eliminado y sus instancias están en proceso de terminación. La solicitud permanece en este estado hasta que se terminen todas las instancias.

`deleted`

La flota de EC2 se elimina y no tiene ninguna instancia de ejecución. La solicitud se elimina dos días después de que todas sus instancias se hayan terminado.

Requisitos previos de flota de EC2

Para crear una flota de EC2, deben existir los requisitos previos siguientes:

- Plantilla de inicialización
- Rol vinculado al servicio de flota de EC2
- Conceder acceso a las claves administradas por el cliente para su uso con AMI cifradas e instantáneas de EBS
- Permisos para los usuarios de la flota de EC2

Plantilla de inicialización

Una plantilla de inicialización incluye información acerca de las instancias que se van a iniciar, como el tipo de instancia, la zona de disponibilidad y el precio máximo que está dispuesto a pagar. Para obtener más información, consulte iniciar una instancia desde una plantilla de inicialización.

Rol vinculado al servicio de flota de EC2

El rol de `AWSServiceRoleForEC2Fleet` concede permiso a la flota de EC2 para solicitar, iniciar, terminar y etiquetar instancias en su nombre. Amazon EC2 utiliza este rol vinculado al servicio para completar las siguientes acciones:

- `ec2:RunInstances`: para iniciar las instancias.
- `ec2:RequestSpotInstances`: solicitar instancias de spot.
- `ec2:TerminateInstances`: para terminar las instancias.
- `ec2:DescribeImages`: describir las imágenes de máquina de Amazon (AMI) para instancias de spot.
- `ec2:DescribeInstanceStatus`: describir el estado de las instancias de spot.
- `ec2:DescribeSubnets`: describir las subredes de las instancias de spot.
- `ec2:CreateTags`: agregar etiquetas a la flota de EC2, instancias y volúmenes.

Asegúrese de que este rol exista antes de utilizar la AWS CLI o una API para crear una flota de EC2.

> **Note**
>
> Una flota de EC2 `instant` no requiere este rol.

Para crear el rol, use la consola de IAM como se indica a continuación.

Para crear el rol AWSServiceRoleForEC2Fleet para la flota de EC2

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, seleccione Roles y luego seleccione Crear rol.
3. En la página Seleccionar tipo de entidad de confianza, haga lo siguiente:
   a. En Tipo de entidad de confianza, elija Servicio de AWS.
   b. En la sección Caso de uso, en Servicio o caso de uso, elija EC2 - Flota.

      > **Tip**
      >
      > Asegúrese de elegir EC2 - Flota. Si elige EC2, el caso de uso EC2 - Flota no aparece en la lista de Caso de uso. El caso de uso EC2 - Flota creará automáticamente una política con los permisos de IAM necesarios y sugerirá AWSServiceRoleForEC2Fleet como nombre del rol.

   c. Elija Siguiente.
4. En la página Agregar permisos, elija Siguiente.
5. En la página Nombrar, revisar y crear, elija Crear rol.

Si ya no tiene que utilizar la flota de EC2, le recomendamos que elimine el rol AWSServiceRoleForEC2Fleet. Después de haber eliminado este rol de la cuenta, podrá volver a crearlo si crea otra flota.

Para obtener más información, consulte Uso de roles vinculados a servicios en la Guía del usuario de IAM.

Conceder acceso a las claves administradas por el cliente para su uso con AMI cifradas e instantáneas de EBS

Si especifica una AMI cifrada o una instantánea de Amazon EBS cifrada en la flota de EC2 y utiliza una clave de AWS KMS para el cifrado, debe conceder permiso al rol AWSServiceRoleForEC2Fleet para que utilice la clave administrada por el cliente a fin de que Amazon EC2 pueda iniciar instancias en su nombre. Para ello, debe agregar una concesión a la clave administrada por el cliente, como se muestra en el siguiente procedimiento.

Al proporcionar permisos, las concesiones son una alternativa a las políticas de claves. Para obtener más información, consulte Uso de concesiones y Uso de políticas de claves en AWS KMS en la Guía para desarrolladores de AWS Key Management Service.

Para conceder permisos al rol AWSServiceRoleForEC2Fleet para que use la clave administrada por el cliente

- Utilice el comando create-grant para agregar una concesión a la clave administrada por el cliente y para especificar la entidad principal (el rol vinculado a un servicio AWSServiceRoleForEC2Fleet) que recibe permiso para realizar las operaciones que permite la concesión. La clave administrada por el cliente se especifica mediante el parámetro `key-id` y el ARN de la clave administrada por el cliente. La entidad principal se especifica con el parámetro `grantee-principal` y el ARN del rol vinculado a un servicio AWSServiceRoleForEC2Fleet.

```
aws kms create-grant \
    --region us-east-1 \
    --key-id arn:aws:kms:us-
east-1:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:role/AWSServiceRoleForEC2Fleet \
    --operations "Decrypt" "Encrypt" "GenerateDataKey"
 "GenerateDataKeyWithoutPlaintext" "CreateGrant" "DescribeKey" "ReEncryptFrom"
 "ReEncryptTo"
```

Permisos para los usuarios de la flota de EC2

Si los usuarios van a crear o administrar una flota de EC2, asegúrese de concederles los permisos necesarios.

Creación de una política para la flota de EC2

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, seleccione Políticas.
3. Elija Crear política.
4. En la página Crear política, elija la pestaña JSON, sustituya el texto por lo siguiente y, a continuación, elija Revisar política.

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
              "iam:ListRoles",
              "iam:PassRole",
              "iam:ListInstanceProfiles"
            ],
            "Resource":"arn:aws:iam::123456789012:role/DevTeam*"
        }
    ]
}
```

`ec2:*` concede a un usuario permiso para llamar a todas las acciones de la API de Amazon EC2. Para limitar las acciones del usuario a unas determinadas acciones de la API de Amazon EC2, especifique dichas acciones.

El usuario debe tener permiso para llamar a la acción `iam:ListRoles` para enumerar los roles de IAM existentes, a la acción `iam:PassRole` para especificar el rol de la flota de EC2 y a la acción `iam:ListInstanceProfiles` para enumerar los perfiles de instancia existentes.

(Opcional) Para permitir a un usuario crear roles o perfiles de instancia mediante la consola de IAM, también tiene que agregar las siguientes acciones a la política:

- `iam:AddRoleToInstanceProfile`
- `iam:AttachRolePolicy`
- `iam:CreateInstanceProfile`
- `iam:CreateRole`
- `iam:GetRole`
- `iam:ListPolicies`

5. En la página Revisar política, escriba un nombre y descripción de política y, a continuación, elija Crear política.
6. Para dar acceso, agregue permisos a los usuarios, grupos o roles:

- Usuarios y grupos en AWS IAM Identity Center:

  Cree un conjunto de permisos. Siga las instrucciones de Creación de un conjunto de permisos en la Guía del usuario de AWS IAM Identity Center.
- Usuarios administrados en IAM a través de un proveedor de identidades:

  Cree un rol para la federación de identidades. Siga las instrucciones descritas en Creación de un rol para un proveedor de identidad de terceros (federación) en la Guía del usuario de IAM.
- Usuarios de IAM:
  - Cree un rol que el usuario pueda aceptar. Siga las instrucciones descritas en Creación de un rol para un usuario de IAM en la Guía del usuario de IAM.
  - (No recomendado) Adjunte una política directamente a un usuario o añada un usuario a un grupo de usuarios. Siga las instrucciones descritas en Adición de permisos a un usuario (consola) de la Guía del usuario de IAM.

Comprobaciones de estado de la flota de EC2

La flota de EC2 comprueba el estado de las instancias de la flota cada dos minutos. El estado de una instancia puede ser `healthy` o `unhealthy`.

La flota de EC2 determina el estado de una instancia a partir de las comprobaciones de estado que proporciona Amazon EC2. Una instancia se determina como `unhealthy` cuando el estado de la comprobación del estado de la instancia o de la comprobación del estado del sistema es `impaired` durante tres comprobaciones de estado de mantenimiento consecutivas. Para obtener más información, consulte Comprobaciones de estado para sus instancias.

Puede configurar la flota para sustituir la Instancias de spot en mal estado. Después de establecer `ReplaceUnhealthyInstances` en `true`, se sustituye una instancia de spot cuando se informa como `unhealthy`. La flota puede ver reducida su capacidad de destino durante unos minutos mientras se sustituye una instancia de spot en mal estado.

Requisitos

- El reemplazo por comprobación de estado se admite solo para flotas de EC2 que mantengan una capacidad de destino (flotas de tipo `maintain`) y no para flotas de tipo `request` o `instant`.
- Solo se admite el reemplazo por comprobación de estado para instancias de spot. Esta función no es compatible con instancias bajo demanda.

- Solo puede configurar una flota de EC2 para sustituir instancias en mal estado al crearla.
- Los usuarios pueden utilizar el reemplazo por comprobación de estado únicamente si tienen permiso para llamar a la acción `ec2:DescribeInstanceStatus`.

Para configurar una flota de EC2 que sustituya instancias de spot en mal estado

1. Siga los pasos para crear una flota de EC2. Para obtener más información, consulte Crear una flota de EC2.
2. Para configurar la flota que sustituya la instancias de spot en mal estado, en el archivo JSON, para `ReplaceUnhealthyInstances`, escriba `true`.

Generar un archivo de configuración JSON de flota de EC2

Para ver la lista completa de los parámetros de configuración de la flota de EC2 puede generar un archivo JSON. Para ver una descripción de cada uno de los parámetros, consulte create-fleet en la referencia de los comandos de la AWS CLI.

Para generar un archivo JSON con todos los parámetros de la flota de EC2 posibles usando la línea de comandos

- Ejecute el comando create-fleet (AWS CLI) y el parámetro `--generate-cli-skeleton` para generar un archivo JSON de flota de EC2 y dirija el resultado a un archivo para guardarlo.

```
aws ec2 create-fleet \
    --generate-cli-skeleton input > ec2createfleet.json
```

Ejemplo de resultado

```
{
    "DryRun": true,
    "ClientToken": "",
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "MaintenanceStrategies": {
            "CapacityRebalance": {
                "ReplacementStrategy": "launch"
            }
        },
        "InstanceInterruptionBehavior": "hibernate",
```

```
        "InstancePoolsToUseCount": 0,
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true,
        "MinTargetCapacity": 0,
        "MaxTotalPrice": ""
    },
    "OnDemandOptions": {
        "AllocationStrategy": "prioritized",
        "CapacityReservationOptions": {
            "UsageStrategy": "use-capacity-reservations-first"
        },
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true,
        "MinTargetCapacity": 0,
        "MaxTotalPrice": ""
    },
    "ExcessCapacityTerminationPolicy": "termination",
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "",
                "LaunchTemplateName": "",
                "Version": ""
            },
            "Overrides": [
                {
                    "InstanceType": "r5.metal",
                    "MaxPrice": "",
                    "SubnetId": "",
                    "AvailabilityZone": "",
                    "WeightedCapacity": 0.0,
                    "Priority": 0.0,
                    "Placement": {
                        "AvailabilityZone": "",
                        "Affinity": "",
                        "GroupName": "",
                        "PartitionNumber": 0,
                        "HostId": "",
                        "Tenancy": "dedicated",
                        "SpreadDomain": "",
                        "HostResourceGroupArn": ""
                    },
                    "InstanceRequirements": {
                        "VCpuCount": {
```

```
                        "Min": 0,
                        "Max": 0
                    },
                    "MemoryMiB": {
                        "Min": 0,
                        "Max": 0
                    },
                    "CpuManufacturers": [
                        "amd"
                    ],
                    "MemoryGiBPerVCpu": {
                        "Min": 0.0,
                        "Max": 0.0
                    },
                    "ExcludedInstanceTypes": [
                        ""
                    ],
                    "InstanceGenerations": [
                        "previous"
                    ],
                    "SpotMaxPricePercentageOverLowestPrice": 0,
                    "OnDemandMaxPricePercentageOverLowestPrice": 0,
                    "BareMetal": "included",
                    "BurstablePerformance": "required",
                    "RequireHibernateSupport": true,
                    "NetworkInterfaceCount": {
                        "Min": 0,
                        "Max": 0
                    },
                    "LocalStorage": "excluded",
                    "LocalStorageTypes": [
                        "ssd"
                    ],
                    "TotalLocalStorageGB": {
                        "Min": 0.0,
                        "Max": 0.0
                    },
                    "BaselineEbsBandwidthMbps": {
                        "Min": 0,
                        "Max": 0
                    },
                    "AcceleratorTypes": [
                        "inference"
                    ],
```

```
                        "AcceleratorCount": {
                            "Min": 0,
                            "Max": 0
                        },
                        "AcceleratorManufacturers": [
                            "amd"
                        ],
                        "AcceleratorNames": [
                            "a100"
                        ],
                        "AcceleratorTotalMemoryMiB": {
                            "Min": 0,
                            "Max": 0
                        }
                    }
                }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 0,
        "OnDemandTargetCapacity": 0,
        "SpotTargetCapacity": 0,
        "DefaultTargetCapacityType": "on-demand",
        "TargetCapacityUnitType": "memory-mib"
    },
    "TerminateInstancesWithExpiration": true,
    "Type": "instant",
    "ValidFrom": "1970-01-01T00:00:00",
    "ValidUntil": "1970-01-01T00:00:00",
    "ReplaceUnhealthyInstances": true,
    "TagSpecifications": [
        {
            "ResourceType": "fleet",
            "Tags": [
                {
                    "Key": "",
                    "Value": ""
                }
            ]
        }
    ],
    "Context": ""
```

```
}
```

Crear una flota de EC2

Para crear una flota de EC2, solo se debe especificar los siguientes parámetros:

- `LaunchTemplateId` o `LaunchTemplateName`: especifica la plantilla de inicialización que se va a utilizar (que contiene los parámetros de las instancias que se van a iniciar, como el tipo de instancia, la zona de disponibilidad y el precio máximo que está dispuesto a pagar)
- `TotalTargetCapacity`: especifica la capacidad objetivo total de la flota
- `DefaultTargetCapacityType`: especifica si la opción de compra predeterminada es bajo demanda o spot

Puede especificar varias especificaciones de inicialización que anulen la plantilla de inicialización. Las especificaciones de inicialización pueden variar según el tipo de instancia, la zona de disponibilidad, la subred y el precio máximo. Además, pueden incluir una capacidad ponderada distinta. Como alternativa, puede especificar los atributos que debe tener una instancia y Amazon EC2 identificará todos los tipos de instancias con esos atributos. Para obtener más información, consulte Selección de tipo de instancia basada en atributos para la flota de EC2.

Si no especifica este parámetro, la flota utiliza el valor predeterminado para el parámetro.

Especifique los parámetros de flota en un archivo JSON. Para obtener más información, consulte Generar un archivo de configuración JSON de flota de EC2.

En este momento, no hay compatibilidad con la consola para crear una flota de EC2.

Para crear una flota de EC2 (AWS CLI)

- Utilice el comando create-fleet (AWS CLI) para crear una flota de EC2 y especificar el archivo JSON que contiene los parámetros de configuración de flota.

```
aws ec2 create-fleet --cli-input-json file://file_name.json
```

Para ver archivos de configuración de ejemplo, consulte Configuraciones de ejemplo de flota de EC2.

A continuación se muestra un resultado de ejemplo para una flota de tipo `request` o `maintain`.

```
{
    "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE"
}
```

A continuación se muestra un resultado de ejemplo para una flota de tipo `instant` que lanzó la capacidad de destino.

```
{
  "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE",
  "Errors": [],
  "Instances": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c5.large",
          "AvailabilityZone": "us-east-1a"
        }
      },
      "Lifecycle": "on-demand",
      "InstanceIds": [
        "i-1234567890abcdef0",
        "i-9876543210abcdef9"
      ],
      "InstanceType": "c5.large",
      "Platform": null
    },
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c4.large",
          "AvailabilityZone": "us-east-1a"
        }
      },
      "Lifecycle": "on-demand",
      "InstanceIds": [
```

```
        "i-5678901234abcdef0",
        "i-5432109876abcdef9"
      ]
  ]
}
```

A continuación se muestra un resultado de ejemplo para una flota de tipo `instant` que lanzó parte de la capacidad de destino con errores para instancias que no se habían iniciado.

```
{
  "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE",
  "Errors": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c4.xlarge",
          "AvailabilityZone": "us-east-1a",
        }
      },
      "Lifecycle": "on-demand",
      "ErrorCode": "InsufficientInstanceCapacity",
      "ErrorMessage": ""
    },
  ],
  "Instances": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c5.large",
          "AvailabilityZone": "us-east-1a"
        }
      },
      "Lifecycle": "on-demand",
      "InstanceIds": [
        "i-1234567890abcdef0",
```

```
        "i-9876543210abcdef9"
      ]
  ]
}
```

A continuación se muestra un resultado de ejemplo para una flota de tipo `instant` que lanzó sin instancias.

```
{
  "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE",
  "Errors": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c4.xlarge",
          "AvailabilityZone": "us-east-1a",
        }
      },
      "Lifecycle": "on-demand",
      "ErrorCode": "InsufficientCapacity",
      "ErrorMessage": ""
    },
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c5.large",
          "AvailabilityZone": "us-east-1a",
        }
      },
      "Lifecycle": "on-demand",
      "ErrorCode": "InsufficientCapacity",
      "ErrorMessage": ""
    },
  ],
  "Instances": []
```

```
}
```

Etiquetar una flota de EC2

Para ayudarle a categorizar y a administrar las solicitudes de flota de EC2, puede etiquetarlas con metadatos personalizados. Puede asignar una etiqueta a una solicitud de flota de EC2 cuando la cree o posteriormente.

Al etiquetar una solicitud de flota, las instancias y volúmenes iniciados por la flota no se etiquetan automáticamente. Tiene que etiquetar explícitamente las instancias y volúmenes iniciados por la flota. Puede elegir asignar etiquetas solo a la solicitud de flota, solo a las instancias iniciadas por la flota, solo a los volúmenes asociados a las instancias iniciadas por la flota o a las tres.

> **Note**
>
> Para los tipos de flota `instant`, puede etiquetar volúmenes asociados a instancias bajo demanda e instancias de spot. Para los tipos de flota `request` o `maintain`, solo puede etiquetar volúmenes asociados a instancias bajo demanda.

Para obtener más información sobre cómo funcionan las etiquetas, consulte Etiquetar los recursos de Amazon EC2.

Requisito previo

Otorgue al usuario el permiso para etiquetar recursos. Para obtener más información, consulte Ejemplo: Etiquetar recursos.

Para conceder a un usuario el permiso para etiquetar recursos

Cree una política de IAM que incluya lo siguiente:

- La acción `ec2:CreateTags`. Esto concede al usuario permiso para crear etiquetas.
- La acción `ec2:CreateFleet`. De esta forma, se concede al usuario permiso para crear una solicitud de flota de EC2.
- Para `Resource`, le recomendamos que especifique `"*"`. Esto permite a los usuarios etiquetar todos los tipos de recursos.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "TagEC2FleetRequest",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags",
                "ec2:CreateFleet"
            ],
            "Resource": "*"
}
```

Important

Actualmente, no admitimos permisos de nivel de recursos para el recurso `create-fleet`. Si especifica `create-fleet` como recurso, obtendrá una excepción no autorizada cuando intente etiquetar la flota. En el ejemplo siguiente se muestra cómo no establecer la política.

```
{
    "Effect": "Allow",
    "Action": [
        "ec2:CreateTags",
        "ec2:CreateFleet"
    ],
    "Resource": "arn:aws:ec2:us-east-1:111122223333:create-fleet/*"
}
```

Para dar acceso, agregue permisos a los usuarios, grupos o roles:

- Usuarios y grupos en AWS IAM Identity Center:

  Cree un conjunto de permisos. Siga las instrucciones de Creación de un conjunto de permisos en la Guía del usuario de AWS IAM Identity Center.

- Usuarios administrados en IAM a través de un proveedor de identidades:

  Cree un rol para la federación de identidades. Siga las instrucciones descritas en Creación de un rol para un proveedor de identidad de terceros (federación) en la Guía del usuario de IAM.

- Usuarios de IAM:

- Cree un rol que el usuario pueda aceptar. Siga las instrucciones descritas en Creación de un rol para un usuario de IAM en la Guía del usuario de IAM.
- (No recomendado) Adjunte una política directamente a un usuario o añada un usuario a un grupo de usuarios. Siga las instrucciones descritas en Adición de permisos a un usuario (consola) de la Guía del usuario de IAM.

Para etiquetar una nueva solicitud de flota de EC2

Para etiquetar una solicitud de flota de EC2 al crearla, especifique el par clave-valor en el archivo JSON utilizado para crear la flota. El valor para `ResourceType` debe ser `fleet`. Si especifica otro valor, la solicitud de flota devuelve un error.

Para etiquetar instancias y volúmenes iniciados por una flota de EC2

Para etiquetar instancias y volúmenes cuando los inicia la flota, especifique las etiquetas en la plantilla de inicialización a la que se hace referencia en la solicitud de flota de EC2.

> **Note**
>
> No puede etiquetar volúmenes asociados a los instancias de spot que se inicien por un tipo de flota `request` o `maintain`.

Para etiquetar una solicitud, una instancia y un volumen de flota de EC2 existentes (AWS CLI)

Utilice el comando create-tags para etiquetar recursos existentes.

```
aws ec2 create-tags \
    --resources fleet-12a34b55-67cd-8ef9-
ba9b-9208dEXAMPLE i-1234567890abcdef0 vol-1234567890EXAMPLE \
    --tags Key=purpose,Value=test
```

Describir la flota de EC2

Puede describir la configuración de la flota de EC2, sus instancias en la flota y el historial de eventos de dicha flota.

Para describir las flotas de EC2 (AWS CLI)

Utilice el comando describe-fleets para describir sus Flotas de EC2.

```
aws ec2 describe-fleets
```

Important

Si una flota es de tipo `instant`, debe especificar el ID de la flota; de lo contrario, no aparece en la respuesta. Incluya `--fleet-ids` de la siguiente manera:

```
aws ec2 describe-fleets --fleet-ids fleet-8a22eee4-f489-ab02-06b8-832a7EXAMPLE
```

Ejemplo de resultado


```
{
    "Fleets": [
        {
            "ActivityStatus": "fulfilled",
            "CreateTime": "2022-02-09T03:35:52+00:00",
            "FleetId": "fleet-364457cd-3a7a-4ed9-83d0-7b63e51bb1b7",
            "FleetState": "active",
            "ExcessCapacityTerminationPolicy": "termination",
            "FulfilledCapacity": 2.0,
            "FulfilledOnDemandCapacity": 0.0,
            "LaunchTemplateConfigs": [
                {
                    "LaunchTemplateSpecification": {
                        "LaunchTemplateName": "my-launch-template",
                        "Version": "$Latest"
                    }
                }
            ],
            "TargetCapacitySpecification": {
                "TotalTargetCapacity": 2,
                "OnDemandTargetCapacity": 0,
                "SpotTargetCapacity": 2,
                "DefaultTargetCapacityType": "spot"
            },
            "TerminateInstancesWithExpiration": false,
            "Type": "maintain",
            "ReplaceUnhealthyInstances": false,
            "SpotOptions": {
                "AllocationStrategy": "capacity-optimized",
```

```
                "InstanceInterruptionBehavior": "terminate"
            },
            "OnDemandOptions": {
                "AllocationStrategy": "lowestPrice"
            }
        }
    ]
}
```

Utilice el comando describe-fleet-instances para describir las instancias de la flota de EC2 especificada. La lista devuelta de instancias en ejecución se actualiza periódicamente y podría no estar actualizada.

```
aws ec2 describe-fleet-instances  --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE
```

Ejemplo de resultado

```
{
    "ActiveInstances": [
        {
            "InstanceId": "i-09cd595998cb3765e",
            "InstanceHealth": "healthy",
            "InstanceType": "m4.large",
            "SpotInstanceRequestId": "sir-86k84j6p"
        },
        {
            "InstanceId": "i-09cf95167ca219f17",
            "InstanceHealth": "healthy",
            "InstanceType": "m4.large",
            "SpotInstanceRequestId": "sir-dvxi7fsm"
        }
    ],
    "FleetId": "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE"
}
```

Utilice el comando describe-fleet-history para describir el historial de la flota de EC2 especificada durante el tiempo indicado.

```
aws ec2 describe-fleet-history --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE --
start-time 2018-04-10T00:00:00Z
```

Ejemplo de resultado


```
{
    "HistoryRecords": [
        {
            "EventInformation": {
                "EventSubType": "submitted"
            },
            "EventType": "fleetRequestChange",
            "Timestamp": "2020-09-01T18:26:05.000Z"
        },
        {
            "EventInformation": {
                "EventSubType": "active"
            },
            "EventType": "fleetRequestChange",
            "Timestamp": "2020-09-01T18:26:15.000Z"
        },
        {
            "EventInformation": {
                "EventDescription": "t2.small, ami-07c8bc5c1ce9598c3, ...",
                "EventSubType": "progress"
            },
            "EventType": "fleetRequestChange",
            "Timestamp": "2020-09-01T18:26:17.000Z"
        },
        {
            "EventInformation": {
                "EventDescription": "{\"instanceType\":\"t2.small\", ...}",
                "EventSubType": "launched",
                "InstanceId": "i-083a1c446e66085d2"
            },
            "EventType": "instanceChange",
            "Timestamp": "2020-09-01T18:26:17.000Z"
        },
        {
            "EventInformation": {
                "EventDescription": "{\"instanceType\":\"t2.small\", ...}",
                "EventSubType": "launched",
                "InstanceId": "i-090db02406cc3c2d6"
            },
            "EventType": "instanceChange",
            "Timestamp": "2020-09-01T18:26:17.000Z"
        }
```

```
    ],
    "FleetId": "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE",
    "LastEvaluatedTime": "1970-01-01T00:00:00.000Z",
    "StartTime": "2018-04-09T23:53:20.000Z"
}
```

Modificar una flota de EC2

Puede modificar una flota de EC2 que se encuentre en el estado `submitted` o `active`. Al modificar una flota, esta pasa al estado `modifying`.

Solo se puede modificar una flota de EC2 que sea de tipo `maintain`. No se puede modificar una flota de EC2 del tipo `request` o `instant`.

Puede modificar los parámetros siguientes de una flota de EC2:

- `target-capacity-specification`: aumenta o reduce la capacidad de destino para `TotalTargetCapacity`, `OnDemandTargetCapacity` y `SpotTargetCapacity`.
- `excess-capacity-termination-policy`: permite indicar si las instancias de ejecución deberán terminarse si se reduce la capacidad de destino total de la flota de EC2 por debajo del tamaño actual de la flota. Los valores válidos son `no-termination` y `termination`.

Cuando se aumenta la capacidad de destino, la flota de EC2 inicia instancias adicionales de acuerdo con la opción de compra de instancias especificada para `DefaultTargetCapacityType`, que pueden ser instancias en diferido o instancias de spot.

Si `DefaultTargetCapacityType` es `spot`, la flota de EC2 inicia las instancias de spot adicionales de acuerdo con su estrategia de asignación.

Cuando se reduce la capacidad de destino, la flota de EC2 elimina todas las solicitudes abiertas que superen la nueva capacidad de destino. Puede solicitar que la flota termine las instancias hasta que el tamaño de la flota alcance la nueva capacidad de destino. Si la estrategia de asignación es `lowest-price`, la flota terminará las instancias con el mayor precio por unidad. Si la estrategia de asignación es `diversified`, la flota terminará instancias de los distintos grupos. También puede solicitar que la flota de EC2 mantenga la flota con su tamaño actual, pero que no sustituya ninguna de las instancias de spot que se hayan interrumpido ni ninguna instancia que el usuario haya terminado manualmente.

Cuando una flota de EC2 termina una instancia de spot porque se ha reducido la capacidad de destino, la instancia recibe un aviso de interrupción de instancia de spot.

Para modificar una flota de EC2 (AWS CLI)

Utilice el comando modify-fleet para actualizar la capacidad de destino de la flota de EC2 especificada.

```
aws ec2 modify-fleet \
    --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --target-capacity-specification TotalTargetCapacity=20
```

Si va a reducir la capacidad de destino pero quiere conservar la flota con su tamaño actual, puede modificar el comando anterior como se indica a continuación.

```
aws ec2 modify-fleet \
    --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --target-capacity-specification TotalTargetCapacity=10 \
    --excess-capacity-termination-policy no-termination
```

Eliminar una flota de EC2

Si ya no necesita una flota de EC2, puede eliminarla. Tras eliminar una flota, todas las solicitudes de spot asociadas con la flota se cancelan, de forma que no se iniciará ninguna instancia de spot nueva.

Al eliminar una flota de EC2, debe especificar si desea terminar también todas sus instancias. Esto incluye tanto las instancias bajo demanda como las instancias de spot. Para las flotas `instant`, la flota de EC2 debe terminar las instancias cuando se elimine la flota. No se admite una flota `instant` eliminada con instancias en ejecución.

Si especifica que se terminen las instancias cuando se elimine la flota, esta pasará al estado `deleted_terminating`. En caso contrario, pasará al estado `deleted_running` y las instancias seguirán ejecutándose hasta que se interrumpan o usted las termine manualmente.

Restricciones

- Puede eliminar hasta 25 flotas del tipo `instant` en una sola solicitud.
- Puede eliminar hasta 100 flotas del tipo `maintain` y `request` en una sola solicitud.
- Puede eliminar hasta 125 flotas en una sola solicitud, siempre que no supere la cuota para cada tipo de flota, como se especificó anteriormente.
- Si supera la cantidad especificada de flotas para eliminar, no se eliminan las flotas.
- Se pueden terminar hasta 1000 instancias en una sola solicitud para eliminar las flotas `instant`.

Para eliminar una flota de EC2 y terminar sus instancias (AWS CLI)

Utilice el comando delete-fleets (eliminar flotas) y el parámetro `--terminate-instances` para eliminar la flota de EC2 especificada y terminar sus instancias asociadas.

```
aws ec2 delete-fleets \
    --fleet-ids fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --terminate-instances
```

Ejemplo de resultado

```
{
    "UnsuccessfulFleetDeletions": [],
    "SuccessfulFleetDeletions": [
        {
            "CurrentFleetState": "deleted_terminating",
            "PreviousFleetState": "active",
            "FleetId": "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE"
        }
    ]
}
```

Para eliminar una flota de EC2 sin terminar sus instancias (AWS CLI)

Puede modificar el comando anterior con el parámetro `--no-terminate-instances` para eliminar la flota de EC2 especificada sin terminar sus instancias asociadas.

> **Note**
>
> `--no-terminate-instances` no es compatible con las flotas `instant`.

```
aws ec2 delete-fleets \
    --fleet-ids fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --no-terminate-instances
```

Ejemplo de resultado

```
{
    "UnsuccessfulFleetDeletions": [],
    "SuccessfulFleetDeletions": [
```

```
        {
            "CurrentFleetState": "deleted_running",
            "PreviousFleetState": "active",
            "FleetId": "fleet-4b8aaae8-dfb5-436d-a4c6-3dafa4c6b7dcEXAMPLE"
        }
    ]
}
```

Solucionar problemas cuando una flota no se puede eliminar

Si una flota de EC2 devuelve un error al eliminarla, `UnsuccessfulFleetDeletions` devuelve el ID de la flota de EC2, un código de error y un mensaje de error.

Los códigos de error son:

- `ExceededInstantFleetNumForDeletion`
- `fleetIdDoesNotExist`
- `fleetIdMalformed`
- `fleetNotInDeletableState`
- `NoTerminateInstancesNotSupported`
- `UnauthorizedOperation`
- `unexpectedError`

Solución de problemas de **`ExceededInstantFleetNumForDeletion`**

Si intenta eliminar más de 25 flotas `instant` en una sola solicitud, se devuelve el error `ExceededInstantFleetNumForDeletion`. A continuación, se muestra un ejemplo del resultado de este error.

```
{
    "UnsuccessfulFleetDeletions": [
     {
          "FleetId": " fleet-5d130460-0c26-bfd9-2c32-0100a098f625",
          "Error": {
                  "Message": "Can’t delete more than 25 instant fleets in a single
 request.",
                  "Code": "ExceededInstantFleetNumForDeletion"
           }
     },
```

```
    {
          "FleetId": "fleet-9a941b23-0286-5bf4-2430-03a029a07e31",
          "Error": {
                "Message": "Can’t delete more than 25 instant fleets in a single
 request.",
                "Code": "ExceededInstantFleetNumForDeletion"
           }
    }
    .
    .
    .
    ],
    "SuccessfulFleetDeletions": []
}
```

Solucionar **NoTerminateInstancesNotSupported**

Si especifica que las instancias de una flota `instant` no deben finalizarse al eliminar la flota, se devuelve el error `NoTerminateInstancesNotSupported`. `--no-terminate-instances` no es compatible con las flotas `instant`. A continuación, se muestra un ejemplo del resultado de este error.

```
{
     "UnsuccessfulFleetDeletions": [
          {
                "FleetId": "fleet-5d130460-0c26-bfd9-2c32-0100a098f625",
                "Error": {
                      "Message": "NoTerminateInstances option is not supported for
 instant fleet",
                      "Code": "NoTerminateInstancesNotSupported"
                 }
          }
      ],
      "SuccessfulFleetDeletions": []
```

Solucionar **UnauthorizedOperation**

Si no tiene permiso para terminar instancias, aparece el error `UnauthorizedOperation` al eliminar una flota que debe terminar sus instancias. La siguiente es la respuesta al error.

```
<Response><Errors><Error><Code>UnauthorizedOperation</Code><Message>You are not
 authorized to perform this
```

```
operation. Encoded authorization failure message: VvuncIxj7Z_CPGNYXWqnuFV-
YjByeAU66Q9752NtQ-I3-qnDLWs6JLFd
KnSMMiq5s6cGqjjPtEDpsnGHzzyHasFHOaRYJpaDVravoW25azn6KNkUQQlFwhJyujt2dtNCdduJfrqcFYAjlEiRMkfDHt7
BHturzDK6A560Y2nDSUiMmAB1y9UNtqaZJ9SNe5sNxKMqZaqKtjRbk02RZu5V2vn9VMk6fm2aMVHbY9JhLvGypLcMUjtJ76
VPiU5v2s-
UgZ7h0p2yth6ysUdhlONg6dBYu8_y_HtEI54invCj4CoK0qawqzMNe6rcmCQHvtCxtXsbkgyaEbcwmrm2m01-
EMhekLFZeJLr
DtYOpYcEl4_nWFX1wtQDCnNNCmxnJZAoJvb3VMDYpDTsxjQv1PxODZuqWHs23YXWVywzgnLtHeRf2o4lUhGBw17mXsS07k7
PT9vrHtQiILor5VVTsjSPWg7edj__1rsnXhwPSu8gI48ZLRGrPQqFq0RmKO_QIE8N8s6NWzCK4yoX-9gDcheurOGpkprPIC
</Message></Error></Errors><RequestID>89b1215c-7814-40ae-a8db-41761f43f2b0</
RequestID></Response>
```

Para resolver el error, debe agregar la acción `ec2:TerminateInstances` a la política de IAM, como se muestra en el siguiente ejemplo.

```
{
       "Version": "2012-10-17",
       "Statement": [
            {
                "Sid": "DeleteFleetsAndTerminateInstances",
                "Effect": "Allow",
                "Action": [
                       "ec2:DeleteFleets"
                       "ec2:TerminateInstances"
                ],
                "Resource": "*"
            }
       ]
   }
```

Flota de spot

Una flota de spot es un conjunto de instancias de spot y, opcionalmente, instancias bajo demanda, que se inicia según los criterios que especifique. La flota de spot selecciona los grupos de capacidad de spot que se ajustan a sus necesidades e inicia instancias de spot para satisfacer la capacidad de destino de la flota. De forma predeterminada, las Flotas de spot se establecen para mantener la capacidad de destino iniciando instancias de reemplazo en cuanto se terminan las instancias de spot de la flota. Puede enviar una flota de spot como una solicitud puntual, que no se conserva una vez que se han terminado las instancias. Puede incluir solicitudes de instancias bajo demanda en una solicitud de flota de spot.

> **Note**
>
> Si quiere usar una consola para crear una flota que incluya instancias de spot, le recomendamos que utilice un grupo de escalado automático en lugar de una flota de spot. Para obtener más información, consulte la sección sobre Grupos de escalado automático con varios tipos de instancia y opciones de compra en la guía del usuario de Amazon EC2 Auto Scaling.
>
> Si quiere usar la AWS CLI para crear una flota que incluya instancias de spot, le recomendamos que utilice un grupo de escalado automático o una flota de EC2 en lugar de una flota de spot. La API RequestSpotFleet, en la que se basa la flota de spot, es una API heredada sin inversión planificada.
>
> Para obtener más información sobre las API de REST recomendadas para utilizar, consulte ¿Cuál es el mejor método de solicitud de spot que se puede utilizar?

Temas

Tipos de solicitudes de flota de spot

Existen dos tipos de solicitudes de flota de spot:

`request`

Si configura el tipo de solicitud como `request`, la flota de spot realiza una solicitud puntual asíncrona para la capacidad deseada. A partir de allí, si la capacidad disminuye debido a interrupciones de spot, la flota no intentará reponer Instancias de spot, ni enviará solicitudes en grupos alternativos de spot si la capacidad no está disponible.

`maintain`

Si configura el tipo de solicitud como `maintain`, la flota de spot realiza una solicitud asíncrona para la capacidad deseada y conserva la capacidad al completar de forma automática las instancias de spot interrumpidas.

Para especificar el tipo de solicitud en la consola de Amazon EC2, haga lo siguiente al crear una solicitud de flota de spot:

- Para crear una flota de spot de tipo `request`, desmarque la casilla Mantener la capacidad de destino.
- Para crear una flota de spot de tipo `maintain`, seleccione la casilla Mantener la capacidad de destino.

Para obtener más información, consulte Creación de una solicitud de flota de spot con los parámetros definidos (consola).

Ambos tipos de solicitudes se benefician de una estrategia de asignación. Para obtener más información, consulte Estrategias de asignación de instancias de spot.

Estrategias de configuración de flota de spot

Una flota de spot es una colección, o flota, de instancias de spot y, opcionalmente, instancias bajo demanda.

La flota de spot intenta iniciar el número de instancias de spot e instancias bajo demanda para ajustarse a la capacidad de destino que haya especificado en la solicitud de flota de spot. La solicitud de instancias de spot se atiende si hay capacidad disponible y el precio máximo especificado en la solicitud es superior al precio de spot actual. Además, la flota de spot puede intentar mantener la capacidad de destino de la flota si las instancias de spot se interrumpen.

También puede establecer la cantidad máxima por hora que está dispuesto a pagar por su flota y la flota de spot inicia instancias hasta que se alcance la cantidad máxima. Cuando se alcanza cantidad

máxima por hora que está dispuesto a pagar, la flota dejará de iniciar instancias, incluso si no se ha alcanzado la capacidad de destino.

Un grupo de capacidad de spot es un conjunto de instancias EC2 no utilizadas con el mismo tipo de instancias (por ejemplo, `m5.large`), sistema operativo, zona de disponibilidad y plataforma de red. Cuando se crea una solicitud de flota de spot, se pueden incluir varias especificaciones de inicialización, que dependen del tipo de instancia, la AMI, la zona de disponibilidad o la subred. La flota de spot selecciona los grupos de capacidad de spot que se usan para atender la solicitud, basándose en las especificaciones de inicialización incluidas es su solicitud de flota de spot y en su configuración. Las Instancias de spot proceden de los grupos seleccionados.

Contenido

Planificación de una solicitud de flota de spot

Antes de crear una solicitud de flota de spot, consulte las Prácticas recomendadas para instancias de spot. Utilice estas prácticas recomendadas cuando planifique su solicitud de flota de spot para aprovisionar el tipo de instancias que desea al menor precio posible. También le recomendamos que realice las siguientes acciones:

- Determine si desea crear una flota de spot que envíe una solicitud única para la capacidad de destino deseada o una que mantenga una capacidad de destino a lo largo del tiempo.
- Determine los tipos de instancias que satisfacen los requisitos de su aplicación.
- Determine la capacidad de destino para la solicitud de flota de spot. Puede definir la capacidad de destino en instancias o en unidades personalizadas. Para obtener más información, consulte Ponderación de instancias de flota de spot.

- Determine qué parte de la capacidad de destino de la flota de spot debe ser capacidad bajo demanda. Puede especificar una capacidad bajo de demanda de 0.
- Determine el precio por unidad, si está usando ponderación de instancias. Para calcular el precio por unidad, divida el precio por hora de instancia entre el número de unidades (o peso) que esta instancia representa. Si no utiliza la ponderación de instancias, el precio por unidad predeterminado es el precio por hora de instancia.
- Revise las posibles opciones para la solicitud de flota de spot. Para obtener más información, consulte el comando request-spot-fleet en la Referencia de comandos de la AWS CLI. Para ver otros ejemplos, consulte Configuraciones de ejemplo de flota de spot.

Estrategias de asignación de instancias de spot

La configuración de inicialización determina todos los grupos de capacidad de spot posibles (tipos de instancias y zonas de disponibilidad) desde los que la flota de spot puede iniciar instancias de spot. Sin embargo, al iniciar instancias, la flota de spot usa la estrategia de asignación que usted especifique para seleccionar los grupos específicos entre todos sus grupos posibles.

> **Note**
>
> (Solo instancias de Linux) Si configura la instancia de spot para lanzarla con la característica SEV-SNP de AMD activada, se le cobrará una tarifa de uso por hora adicional que equivale al 10 % de la tarifa horaria bajo demanda del tipo de instancia seleccionado. Si la estrategia de asignación utiliza el precio como variable, la flota de EC2 no incluye esta tarifa adicional; solo se utiliza el precio de spot.

Estrategias de asignación

Puede especificar una de las siguientes estrategias de asignación para sus instancias de spot:

`priceCapacityOptimized` (recomendado)

La flota de spot identifica los grupos con la mayor disponibilidad de capacidad para la cantidad de instancias que se van a lanzar. Esto significa que solicitaremos instancias de spot de los grupos que consideremos que tienen menos probabilidades de interrupción a corto plazo. A continuación, la flota de spot solicita instancias de spot de los grupos con el precio más bajo.

La estrategia de asignación de `priceCapacityOptimized` es la mejor opción para la mayoría de las cargas de trabajo de spot, como las aplicaciones en contenedores sin estado, los microservicios, las aplicaciones web, los trabajos de datos y análisis y el procesamiento por lotes.

`capacityOptimized`

La flota de spot identifica los grupos con la mayor disponibilidad de capacidad para la cantidad de instancias que se van a lanzar. Esto significa que solicitaremos instancias de spot de los grupos que consideremos que tienen menos probabilidades de interrupción a corto plazo. Opcionalmente, puede establecer una prioridad para cada tipo de instancia de su flota utilizando `capacityOptimizedPrioritized`. La flota de spot optimiza la capacidad en primer lugar, pero respeta las prioridades de los tipos de instancias sobre la base del mejor esfuerzo.

Con las instancias de spot, los precios cambian lentamente con el paso del tiempo en función de las tendencias a largo plazo de la oferta y la demanda, pero la capacidad fluctúa en tiempo real. La estrategia `capacityOptimized` inicia instancias de spot de forma automática en los grupos con mayor disponibilidad, analizando los datos de capacidad en tiempo real y prediciendo cuáles son los que tienen una mayor disponibilidad. Esto funciona bien para las cargas de trabajo que pueden tener un costo mayor de interrupción asociado al reinicio del trabajo, como integración continua (CI) prolongada, representación de imágenes y medios, aprendizaje profundo y computación de alto rendimiento (HPC) que pueden tener un costo mayor de interrupción asociado al reinicio del trabajo. Al ofrecer la posibilidad de experimentar menos interrupciones, la estrategia `capacityOptimized` puede reducir el costo total de la carga de trabajo.

Como alternativa, puede utilizar la estrategia de asignación `capacityOptimizedPrioritized` con un parámetro de prioridad para ordenar los tipos de instancias de la prioridad más alta a la más baja. Puede establecer la misma prioridad para diferentes tipos de instancia. La flota de spot optimizará primero la capacidad, pero respetará las prioridades de tipo de instancias sobre la base del mejor esfuerzo (por ejemplo, si el respeto de las prioridades no afecta significativamente la capacidad de la flota de spot para aprovisionar la capacidad óptima). Esta es una buena opción para cargas de trabajo en las que se debe minimizar la posibilidad de interrupción y también importa la preferencia por ciertos tipos de instancias. El uso de prioridades solo se admite si la flota utiliza una plantilla de inicialización. Tenga en cuenta que cuando establece la prioridad para `capacityOptimizedPrioritized`, la misma prioridad también se aplica a las instancias bajo demanda si `AllocationStrategy` bajo demanda se establece en `prioritized`.

`diversified`

Las instancias de spot se distribuyen entre todos los grupos.

Elegir una estrategia de asignación adecuada

Para poder optimizar su flota para su caso de uso, elija la estrategia de asignación de spot adecuada. Para garantizar la capacidad de destino de las instancias bajo demanda, la flota de spot siempre selecciona el tipo de instancia menos costoso en función del precio de las instancias bajo demanda públicas, pero siempre se ciñe a la estrategia de asignación (ya sea `priceCapacityOptimized`, `capacityOptimized` o `diversified`) de las instancias de spot.

Equilibrio del precio más bajo y la disponibilidad de capacidad

Para equilibrar las compensaciones entre los grupos de capacidad de spot con el precio más bajo y los grupos de capacidad de spot con la mayor disponibilidad de capacidad, le recomendamos utilizar la estrategia de asignación `priceCapacityOptimized`. Esta estrategia toma decisiones sobre a qué grupos se van a solicitar instancias de spot en función del precio de los grupos y de la disponibilidad de capacidad de las instancias de spot de esos grupos. Esto significa que solicitaremos instancias de spot a los grupos que consideremos que tienen la menor probabilidad de interrupción a corto plazo, sin dejar de tener en cuenta el precio.

Si la flota ejecuta cargas de trabajo resistentes y sin estado, como aplicaciones en contenedores, microservicios, aplicaciones web, trabajos de datos y análisis y procesamiento por lotes, utilice la estrategia de asignación `priceCapacityOptimized` para obtener ahorros de costos y disponibilidad de capacidad óptimos.

Si la flota ejecuta cargas de trabajo que pueden tener un costo mayor de interrupción asociado al reinicio del trabajo, debe implementar puntos de control para que las aplicaciones puedan reiniciarse desde ese punto en caso de que se interrumpan. Al utilizar puntos de control, la estrategia de asignación `priceCapacityOptimized` es una buena opción para estas cargas de trabajo, ya que asigna capacidad de los grupos con el precio más bajo y, además, ofrecen una tasa de interrupción de instancia de spot baja.

Para ver un ejemplo de configuración que utiliza la estrategia de asignación `priceCapacityOptimized`, consulte Ejemplo 9: lanzamiento de instancias de spot en una flota de capacidad optimizada con prioridades.

Cuando las cargas de trabajo tienen un alto costo de interrupción

Si lo desea, puede utilizar la estrategia `capacityOptimized` si ejecuta cargas de trabajo que utilizan tipos de instancias con precios similares o si el costo de la interrupción es tan importante que cualquier ahorro de costos es insuficiente en comparación con un aumento marginal de las interrupciones. Esta estrategia asigna capacidad de los grupos de capacidad de spot de la mayor

disponibilidad que ofrecen la posibilidad de sufrir menos interrupciones, lo que puede reducir el costo total de la carga de trabajo. Para ver un ejemplo de configuración que utiliza la estrategia de asignación `capacityOptimized`, consulte Ejemplo 7: configuración del reequilibrio de capacidad para iniciar instancias de spot de reemplazo.

Cuando se debe minimizar la posibilidad de interrupción, pero la preferencia por determinados tipos de instancia es importante, puede expresar las prioridades del grupo mediante la estrategia de asignación `capacityOptimizedPrioritized` y, luego, establecer el orden de los tipos de instancias que se utilizarán, de la prioridad más alta a la más baja. Para ver una configuración de ejemplo, consulte Ejemplo 8: inicialización de instancias de spot en una flota de capacidad optimizada.

Tenga en cuenta que el uso de prioridades solo se admite si la flota utiliza una plantilla de inicialización. También tenga en cuenta que, cuando establece prioridades para `capacityOptimizedPrioritized`, estas también se aplican a las instancias bajo demanda si `AllocationStrategy` bajo demanda se establece en `prioritized`.

Cuando su carga de trabajo es flexible en el tiempo y la disponibilidad de la capacidad no es un factor

Si una flota es pequeña o se ejecuta durante poco tiempo, puede utilizar `priceCapacityOptimized` para maximizar el ahorro de costos sin dejar de tener en cuenta la disponibilidad de capacidad.

Cuando la flota es grande o se ejecuta durante mucho tiempo

Si la flota es grande o se ejecuta durante mucho tiempo, puede mejorar su disponibilidad al distribuir las instancias de spot entre varios grupos, al usar la estrategia `diversified`. Por ejemplo, si la flota de spot especifica 10 grupos y una capacidad de destino de 100 instancias, la flota inicia 10 instancias de spot en cada grupo. Si el precio de spot de un grupo sobrepasa el precio máximo de ese grupo, solo el 10 % de la flota se ve afectada. El uso de esta estrategia también consigue que su flota sea menos sensible a los aumentos en el precio de spot en cualquiera de los grupos a lo largo del tiempo. Con la estrategia `diversified`, la flota de spot no inicia instancias de spot; en ningún grupo con un precio de spot que sea mayor o igual que el precio bajo demanda.

Mantener la capacidad de destino

Después de que las instancias de spot se terminen debido a un cambio en el precio de spot o en la capacidad disponible de un grupo de capacidad de spot, una flota de spot de tipo `maintain` inicia

las instancias de spot de reemplazo. La estrategia de asignación determina los grupos desde los que se lanzan las instancias de reemplazo, de la siguiente manera:

- Si la estrategia de asignación es `priceCapacityOptimized`, la flota inicia instancias de reemplazo en los grupos que tienen la mayor disponibilidad de capacidad de instancia de spot, sin dejar de tener en cuenta el precio e identifica los grupos con el precio más bajo con alta disponibilidad de capacidad.
- Si la estrategia de asignación es `capacityOptimized`, la flota inicia instancias de reemplazo en los grupos que tienen la mayor disponibilidad de capacidad de instancia de spot.
- Si la estrategia de asignación es `diversified`, la flota distribuye las instancias de spot de reemplazo entre los grupos restantes.

Selección de tipo de instancia basada en atributos para la flota de spot

Al crear una flota de spot, debe especificar uno o varios tipos de instancias para configurar las instancias bajo demanda y las instancias de spot en la flota. Como alternativa a especificar de forma manual los tipos de instancia, puede especificar los atributos que debe tener una instancia y Amazon EC2 identificará todos los tipos de instancias con esos atributos. Esto se conoce como selección de tipo de instancia basada en atributos. Por ejemplo, puede especificar el número mínimo y máximo de vCPU necesarias para sus instancias y la flota de spot iniciará las instancias mediante cualquier tipo de instancia disponible que cumpla con esos requisitos de vCPU.

La selección de tipo de instancia basada en atributos es ideal para cargas de trabajo y marcos que pueden ser flexibles sobre los tipos de instancias que utilizan, como cuando se ejecutan contenedores o flotas web, se procesan macrodatos y se implementan herramientas de integración e implementación continuas (CI/CD).

Beneficios

La selección de tipo de instancia basada en atributos posee los siguientes beneficios:

- Uso fácil de los tipos de instancias correctos: con tantos tipos de instancias disponibles, encontrar los tipos de instancias adecuados para su carga de trabajo puede necesitar mucho tiempo. Cuando especifica atributos de instancia, los tipos de instancia tendrán automáticamente los atributos necesarios para la carga de trabajo.
- Configuración simplificada: para especificar de forma manual varios tipos de instancias para una flota de spot, debe crear una anulación de la plantilla de inicialización independiente para cada tipo de instancia. Sin embargo, con la selección de tipo de instancia basada en atributos, para

proporcionar varios tipos de instancias solo necesita especificar los atributos de instancia en la plantilla de lanzamiento o en una anulación de la plantilla de lanzamiento.

- Uso automático de nuevos tipos de instancias: cuando se especifican atributos de instancia en lugar de tipos de instancias, su flota puede utilizar tipos de instancias de nueva generación a medida que se publican, con lo que se prueba la eficiencia futura de la configuración de la flota.
- Flexibilidad del tipo de instancias: cuando se especifican atributos de instancias en lugar de tipos de instancias, la flota de spot puede seleccionar entre una amplia gama de tipos de instancias para iniciar instancias de spot, de forma que se siguen las prácticas recomendadas de instancias de spot de flexibilidad con respecto a los tipos de instancia.

Temas

Cómo funciona la selección de tipo de instancia basada en atributos

Para utilizar la selección de tipo de instancia basada en atributos en la configuración de la flota, debe reemplazar la lista de tipos de instancias por una lista de atributos de instancia que requieren las instancias. La flota de spot iniciará instancias en cualquier tipo de instancia disponible que tenga los atributos de instancia especificados.

Temas

Tipos de atributos de instancia

Hay varios atributos de instancia que puede especificar para expresar los requisitos de computación, como, por ejemplo:

- Recuento de vCPU: el número mínimo y máximo de vCPU por instancia.
- Memoria: los GiB de memoria mínimos y máximos por instancia.
- Almacenamiento local: si se usarán volúmenes de almacén de instancias o EBS para el almacenamiento local.
- Rendimiento ampliable: si se usará la familia de instancias T, incluidos los tipos T4g, T3a, T3 y T2.

Para obtener una descripción de cada atributo y los valores predeterminados, consulte InstanceRequirements en la Referencia de la API de Amazon EC2.

Dónde configurar la selección de tipo de instancia basada en atributos

Según si utiliza la consola o la AWS CLI, puede especificar los atributos de instancia para la selección de tipo de instancia basada en atributos de la siguiente manera:

En la consola, puede especificar los atributos de instancia en uno o ambos de los siguientes componentes de configuración de la flota:

- En una plantilla de inicialización y, luego, hacer referencia a la plantilla de inicialización en la solicitud de flota.
- En la solicitud de flota

En la AWS CLI puede especificar los atributos de la instancia en uno o todos los siguientes componentes de configuración de la flota:

- En una plantilla de inicialización, y hacer referencia a la plantilla de inicialización en la solicitud de flota.
- En una anulación de la plantilla de inicialización

  Si desea una combinación de instancias que utilizan diferentes AMI, puede especificar atributos de instancia en varias anulaciones de plantillas de lanzamiento. Por ejemplo, distintos tipos de instancias pueden utilizar procesadores x86 y basados en Arm.
- En una especificación de lanzamiento

Cómo utiliza la flota de spot la selección de tipo de instancia basada en atributos al aprovisionar una flota

La flota de spot aprovisiona una flota de la siguiente manera:

- La flota de spot identifica los tipos de instancias que tienen los atributos especificados.
- La flota de spot utiliza la protección de precios para determinar qué tipos de instancias excluir.
- La flota de spot determina los grupos de capacidad desde los que considerará iniciar las instancias en función de las regiones de AWS o zonas de disponibilidad que tienen tipos de instancias coincidentes.
- La flota de spot aplica la estrategia de asignación especificada para determinar desde qué grupos de capacidad se van a iniciar las instancias.

  Tenga en cuenta que la selección de tipo de instancia basada en atributos no selecciona los grupos de capacidad desde los que se aprovisiona la flota; eso depende de las estrategias de asignación. Puede que haya un gran número de tipos de instancias con atributos especificados, y algunos de ellos pueden ser costosos.

  Si especifica una estrategia de asignación, la flota de spot lanzará instancias de acuerdo con la estrategia de asignación especificada.

  - Para las instancias de spot, la selección de tipo de instancia basada en atributos admite las estrategias de asignación `capacityOptimizedPrioritized` y `capacityOptimized`.
  - Para las instancias bajo demanda, la selección del tipo de instancia basada en atributos admite la estrategia de asignación de `lowestPrice`, lo que garantiza que la flota de spot iniciará instancias bajo demanda de los grupos de capacidad menos costosos.
- Si no hay capacidad para los tipos de instancias con los atributos de instancia especificados, no se pueden lanzar instancias y la flota devuelve un error.

Protección de precios

La protección de precios es una característica que impide que su flota de spot utilice tipos de instancias que consideraría demasiado caros, incluso si se ajustan a los atributos especificados. Para utilizar la protección de precios, debe establecer un umbral de precios. A continuación, cuando Amazon EC2 selecciona tipos de instancias con sus atributos, excluye los tipos de instancias con precios superiores al umbral.

La forma en que Amazon EC2 calcula el umbral de precio es la siguiente:

- En primer lugar, Amazon EC2 identifica el tipo de instancia con el precio más bajo entre los que coinciden con sus atributos.

- A continuación, Amazon EC2 toma el valor (expresado como porcentaje) que especificó para el parámetro de protección de precios y lo multiplica por el precio del tipo de instancias identificado. El resultado es el precio que se utiliza como umbral de precio.

Existen límites de precios diferentes para las instancias bajo demanda y las instancias de spot.

Cuando crea una flota con la selección del tipo de instancia basada en atributos, se habilita la protección de precios de forma predeterminada. Puede mantener los valores predeterminados o especificar los suyos.

También puede desactivar la protección de precios. Para indicar que no hay umbral de protección de precios, especifique un valor de porcentaje alto, como 999999.

Temas

Cómo se identifica el tipo de instancia con el precio más bajo

Amazon EC2 determina el precio en el que se basará el umbral de precios mediante la identificación del tipo de instancia con el precio más bajo entre los que coinciden con los atributos especificados. Lo hace de la siguiente forma:

- En primer lugar, analiza los tipos de instancias C, M o R de la generación actual que coincidan con sus atributos. Si encuentra alguna coincidencia, identifica el tipo de instancia con el precio más bajo.
- Si no hay ninguna coincidencia, analiza los tipos de instancias de la generación actual que coincidan con sus atributos. Si encuentra alguna coincidencia, identifica el tipo de instancia con el precio más bajo.
- Si no hay ninguna coincidencia, analiza los tipos de instancias de la generación anterior que coincidan con sus atributos e identifica el tipo de instancia con el precio más bajo.

Protección de precios de las instancias bajo demanda

El umbral de protección de precios para los tipos de instancias bajo demanda se calcula como un porcentaje superior al tipo de instancia bajo demanda identificado con el precio más bajo (`OnDemandMaxPricePercentageOverLowestPrice`). Especificará el porcentaje más alto que está dispuesto a pagar. Si no especifica este parámetro, se utilizará el valor predeterminado `20` para calcular un umbral de protección de precios superior en un 20 % al precio identificado.

Por ejemplo, si el precio de la instancia bajo demanda identificada es `0.4271` y usted especificó `25`, el umbral de precios es un 25 % superior a `0.4271`. Se calcula como se indica a continuación: `0.4271 * 1.25 = 0.533875`. El precio calculado es el máximo que está dispuesto a pagar por las instancias bajo demanda y, en este ejemplo, Amazon EC2 excluirá cualquier tipo de instancia bajo demanda que cueste más de `0.533875`.

Protección de precios de instancias de spot

De manera predeterminada, Amazon EC2 aplicará automáticamente una protección óptima del precio de las instancias de spot para seleccionar de manera coherente entre una amplia gama de tipos de instancia. También puede configurar manualmente la protección de precios. Sin embargo, dejar que Amazon EC2 lo haga puede aumentar la probabilidad de que se agote la capacidad de spot.

Puede especificar manualmente la protección de precios con una de las opciones siguientes. Si configura manualmente la protección de precios, le recomendamos utilizar la primera opción.

- Un porcentaje del tipo de instancia bajo demanda identificado con el precio más bajo [`MaxSpotPriceAsPercentageOfOptimalOnDemandPrice`]

  Por ejemplo, si el precio del tipo de instancia bajo demanda identificado es `0.4271` y usted especificó `60`, el umbral de precios es un 60 % de `0.4271`. Se calcula como se indica a continuación: `0.4271 * 0.60 = 0.25626`. El precio calculado es el máximo que está dispuesto a pagar por las instancias de spot y, en este ejemplo, Amazon EC2 excluirá cualquier tipo de instancia de spot que cueste más de `0.25626`.
- Un porcentaje superior al tipo de instancia de spot identificado con el precio más bajo [`SpotMaxPricePercentageOverLowestPrice`]

  Por ejemplo, si el precio del tipo de instancia de spot identificado es `0.1808` y usted especificó `25`, el umbral de precios es un 25 % superior a `0.1808`. Se calcula como se indica a continuación: `0.1808 * 1.25 = 0.226`. El precio calculado es el máximo que está dispuesto a pagar por las

instancias de spot y, en este ejemplo, Amazon EC2 excluirá cualquier tipo de instancia de spot que cueste más de `0.266`. No le recomendamos utilizar este parámetro porque los precios de spot pueden fluctuar y, por lo tanto, su umbral de protección de precios también puede fluctuar.

Especificación del umbral de protección de precios

Para especificar el límite de protección de precios

Cuando cree la flota de spot, configure la flota para la selección del tipo de instancia basada en atributos y, a continuación, haga lo siguiente:

- Consola

  Para especificar el límite de protección de precios de las instancias bajo demanda, en Atributo de instancia adicional, elija Protección de precios bajo demanda y, luego, elija Agregar atributo. En Porcentaje de protección de precios bajo demanda, ingrese el límite de protección de precios en forma de porcentaje.

  Para especificar el límite de protección de precios de las instancias de spot, en Atributo de instancia adicional, elija Protección de precios de spot y luego elija Agregar atributo. Elija un parámetro e ingrese el umbral de protección de precios en forma de porcentaje.
- AWS CLI

  Para especificar el límite de protección de precios de las instancias bajo demanda, en el archivo de configuración JSON, en la estructura `InstanceRequirements`, en `OnDemandMaxPricePercentageOverLowestPrice`, ingrese el límite de protección de precios en forma de porcentaje.

  Para especificar el umbral de protección de precios de las instancias de spot, en el archivo de configuración JSON, en la estructura `InstanceRequirements`, especifique uno de los siguientes parámetros:
  - En `MaxSpotPriceAsPercentageOfOptimalOnDemandPrice`, ingrese el umbral de protección de precios en forma de porcentaje.
  - En `SpotMaxPricePercentageOverLowestPrice`, ingrese el umbral de protección de precios en forma de porcentaje.

Para obtener más información sobre la creación de una flota, consulte Cree una flota de spot con la selección de tipo de instancia basada en atributos.

> **Note**
>
> Cuando se crea la flota de spot, si se establece el tipo Capacidad de destino total como vCPUs o Memoria (MiB) (consola), o bien `TargetCapacityUnitType` como `vcpu` o `memory-mib` (AWS CLI), el límite de protección de precios se aplica en función del precio por vCPU o por memoria, en lugar del precio por instancia.

Consideraciones

- Puede especificar tipos de instancias o atributos de instancia en una flota de spot, pero no ambos al mismo tiempo.

  Al utilizar la CLI, las anulaciones de la plantilla de lanzamiento anularán la plantilla de lanzamiento. Por ejemplo, si la plantilla de inicialización contiene un tipo de instancia y la anulación de la plantilla de inicialización contiene atributos de instancia, las instancias identificadas por los atributos de instancia anularán el tipo de instancia en la plantilla de inicialización.
- Al utilizar la CLI, cuando especifica atributos de instancia como anulaciones, no puede especificar ponderaciones ni prioridades al mismo tiempo.
- Puede especificar un máximo de cuatro estructuras `InstanceRequirements` en una configuración de solicitud.

Cree una flota de spot con la selección de tipo de instancia basada en atributos

Puede configurar una flota para utilizar la selección de tipo de instancia basada en atributos mediante la consola de Amazon EC2 o la AWS CLI.

Temas

- Creación de una flota de spot mediante la consola
- Creación de una flota de spot mediante la AWS CLI

Creación de una flota de spot mediante la consola

Para configurar una flota de spot para la selección de tipo de instancia basada en atributos (consola)

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

2. En el panel de navegación, elija Solicitudes de spot y, a continuación, elija Solicitar instancias de spot.
3. Siga los pasos para crear una flota de spot. Para obtener más información, consulte Creación de una solicitud de flota de spot con los parámetros definidos (consola).

   Al crear la flota de spot, configure la flota para la selección de tipo de instancia basada en atributos de la siguiente manera:

   a. En Requisitos de tipo de instancia, elija Especificar los atributos de instancia que coinciden con los requisitos de computación.
   b. En vCPU, ingrese el número mínimo y máximo deseado de vCPU. Para no especificar ningún límite, seleccione No minimum (Sin mínimo), No maximum (Sin máximo) o ambos.
   c. En Memory (GiB) (Memoria [GiB]), ingrese la cantidad mínima y máxima de memoria deseada. Para no especificar ningún límite, seleccione No minimum (Sin mínimo), No maximum (Sin máximo) o ambos.
   d. (Opcional) En Additional instance attributes (Atributos de instancia adicionales), puede especificar opcionalmente uno o varios atributos para expresar sus requisitos de computación con más detalle. Cada atributo adicional agrega más restricciones a la solicitud.
   e. (Opcional) Expanda Vista previa de tipos de instancia coincidentes para ver los tipos de instancias que tienen los atributos especificados.

Creación de una flota de spot mediante la AWS CLI

Para configurar una flota de spot para la selección de tipo de instancia basada en atributos (AWS CLI)

Utilice el comando request-spot-fleet (AWS CLI) para crear una flota de spot. Especifique la configuración de la flota en un archivo JSON.

```
aws ec2 request-spot-fleet \
    --region us-east-1 \
    --spot-fleet-request-config file://file_name.json
```

Archivo *file_name*.json de ejemplo

En el siguiente ejemplo, se incluyen los parámetros que configuran una flota de spot para utilizar la selección de tipos de instancia basada en atributos y va seguida de una explicación de texto.

```
{
 "AllocationStrategy": "priceCapacityOptimized",
 "TargetCapacity": 20,
 "Type": "request",
 "LaunchTemplateConfigs": [{
  "LaunchTemplateSpecification": {
   "LaunchTemplateName": "my-launch-template",
   "Version": "1"
  },
  "Overrides": [{
   "InstanceRequirements": {
    "VCpuCount": {
     "Min": 2
    },
    "MemoryMiB": {
     "Min": 4
    }
   }
  }]
 }]
}
```

Los atributos para la selección de tipos de instancia basada en atributos se especifican en la estructura `InstanceRequirements`. En este ejemplo, se especifican dos atributos:

- `VCpuCount`: se especifica un mínimo de 2 vCPU. Como no se especifica ningún máximo, no hay ningún límite máximo.
- `MemoryMiB`: se especifica un mínimo de 4 MiB de memoria. Como no se especifica ningún máximo, no hay ningún límite máximo.

Se identificarán los tipos de instancia que tengan 2 o más vCPU y 4 MiB o más de memoria. Sin embargo, la protección de precios y la estrategia de asignación pueden excluir algunos tipos de instancias cuando la flota de spot aprovisiona la flota.

Para obtener una lista y descripciones de todos los atributos posibles que se pueden especificar, consulte InstanceRequirements en la Referencia de la API de Amazon EC2.

> **Note**
>
> Cuando `InstanceRequirements` se incluye en la configuración de la flota, `InstanceType` y `WeightedCapacity` deben excluirse; no pueden determinar la configuración de la flota al mismo tiempo que los atributos de instancia.

El objeto JSON también contiene la siguiente configuración de flota:

- `"AllocationStrategy": "priceCapacityOptimized"`: la estrategia de asignación de las instancias de spot de la flota.
- `"LaunchTemplateName": "my-launch-template", "Version": "1"`: la plantilla de inicialización contiene información sobre la configuración de las instancias, pero, si se especifican los tipos de instancias, se anularán con los atributos especificados en `InstanceRequirements`.
- `"TargetCapacity": 20`: la capacidad de destino es de 20 instancias.
- `"Type": "request"`: el tipo de solicitud para la flota es `request`.

Ejemplos de configuraciones válidas y no válidas

Si utiliza la AWS CLI para crear una flota de spot, debe asegurarse de que la configuración de la flota sea válida. En los siguientes ejemplos, se muestran configuraciones válidas y no válidas.

Las configuraciones no se consideran válidas cuando contienen lo siguiente:

- Una única estructura `Overrides` con `InstanceRequirements` y `InstanceType` a la vez
- Dos estructuras `Overrides`, una con `InstanceRequirements` y la otra con `InstanceType`
- Dos estructuras `InstanceRequirements` con valores de atributo superpuestos dentro de la misma `LaunchTemplateSpecification`

Configuraciones de ejemplo

- Configuración válida: plantilla de inicialización única con anulaciones
- Configuración válida: plantilla de lanzamiento única con varios requisitos de instancia
- Configuración válida: dos plantillas de inicialización, cada una con anulaciones
- Configuración válida: solo InstanceRequirements especificado, sin valores de atributo superpuestos

- La configuración no es válida: Overrides contiene InstanceRequirements y InstanceType
- La configuración no es válida: dos Overrides contienen InstanceRequirements y InstanceType
- La configuración no es válida: valores de atributo superpuestos

Configuración válida: plantilla de inicialización única con anulaciones

La siguiente configuración es válida. Contiene una plantilla de inicialización y otra estructura `Overrides` que contiene una estructura `InstanceRequirements`. A continuación, se presenta una explicación de texto de la configuración de ejemplo.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "My-launch-template",
                "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 2,
                            "Max": 8
                        },
                        "MemoryMib": {
                            "Min": 0,
                            "Max": 10240
                        },
                        "MemoryGiBPerVCpu": {
                            "Max": 10000
                        },
                        "RequireHibernateSupport": true
                    }
                }
            ]
        }
    ],
```

```
        "TargetCapacity": 5000,
            "OnDemandTargetCapacity": 0,
            "TargetCapacityUnitType": "vcpu"
    }
}
```

`InstanceRequirements`

Para utilizar la selección de instancias basada en atributos, debe incluir la estructura `InstanceRequirements` en la configuración de la flota y especificar los atributos deseados para las instancias de la flota.

En el ejemplo anterior, se especifican los siguientes atributos de instancia:

- `VCpuCount`: los tipos de instancia deben tener un mínimo de 2 y un máximo de 8 vCPU.
- `MemoryMiB`: los tipos de instancia deben tener un máximo de 10 240 MiB de memoria. Un mínimo de 0 indica que no hay un límite mínimo.
- `MemoryGiBPerVCpu`: los tipos de instancia deben tener un máximo de 10 000 GiB de memoria por vCPU. El parámetro `Min` es opcional. Al omitirlo, indica que no hay un límite mínimo.

`TargetCapacityUnitType`

El parámetro `TargetCapacityUnitType` especifica la unidad de la capacidad de destino. En el ejemplo, la capacidad objetivo es `5000` y el tipo de unidad de capacidad objetivo es `vcpu`, que en conjunto especifican una capacidad de destino deseada de 5000 vCPU. La flota de spot iniciará suficientes instancias para que el número total de vCPU de la flota sea de 5000 vCPU.

Configuración válida: plantilla de lanzamiento única con varios requisitos de instancia

La siguiente configuración es válida. Contiene una plantilla de inicialización y una estructura `Overrides` que contiene dos estructuras `InstanceRequirements`. Los atributos especificados en `InstanceRequirements` son válidos porque los valores no se superponen; la primera estructura `InstanceRequirements` especifica un `VCpuCount` de 0 a 2 vCPU, mientras que la segunda estructura `InstanceRequirements` especifica de 4 a 8 vCPU.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
```

```
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 4,
                            "Max": 8
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Configuración válida: dos plantillas de inicialización, cada una con anulaciones

La siguiente configuración es válida. Contiene dos plantillas de inicialización, cada una con una estructura `Overrides` que contiene una estructura `InstanceRequirements`. Esta configuración resulta útil para el soporte de arquitectura `arm` y `x86` en la misma flota.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "armLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "x86LaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
```

```
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Configuración válida: solo **`InstanceRequirements`** especificado, sin valores de atributo superpuestos

La siguiente configuración es válida. Contiene dos estructuras `LaunchTemplateSpecification`, cada una con una plantilla de inicialización y una estructura `Overrides` que contiene una estructura `InstanceRequirements`. Los atributos especificados en `InstanceRequirements` son válidos porque los valores no se superponen; la primera estructura `InstanceRequirements` especifica un `VCpuCount` de 0 a 2 vCPU, mientras que la segunda estructura `InstanceRequirements` especifica de 4 a 8 vCPU.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
```

```
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            },
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyOtherLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 4,
                            "Max": 8
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

La configuración no es válida: **`Overrides`** contiene **`InstanceRequirements`** y **`InstanceType`**

La siguiente configuración no es válida. La estructura `Overrides` contiene tanto `InstanceRequirements` como `InstanceType`. En `Overrides`, puede especificar `InstanceRequirements` o `InstanceType`, pero no ambos.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
```

```
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                    "InstanceType": "m5.large"
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

La configuración no es válida: dos **`Overrides`** contienen **`InstanceRequirements`** y **`InstanceType`**

La siguiente configuración no es válida. Las estructuras `Overrides` contienen tanto `InstanceRequirements` como `InstanceType`. Puede especificar `InstanceRequirements` o `InstanceType`, pero no ambos, incluso si están en diferentes estructuras `Overrides`.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
```

```
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            },
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyOtherLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceType": "m5.large"
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

La configuración no es válida: valores de atributo superpuestos

La siguiente configuración no es válida. Cada una de las dos estructuras `InstanceRequirements` contienen `"VCpuCount": {"Min": 0, "Max": 2}`. Los valores de estos atributos se superponen, lo que dará lugar a grupos de capacidad duplicados.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    },
                    {
                      "InstanceRequirements": {
                          "VCpuCount": {
                              "Min": 0,
                              "Max": 2
                          },
                          "MemoryMiB": {
                              "Min": 0
                          }
                      }
                  }
                }
              ]
            }
```

```
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Vista previa de tipos de instancia con atributos especificados

Puede utilizar el comando de la AWS CLI get-instance-types-from-instance-requirements para obtener una vista previa de los tipos de instancias que coinciden con los atributos especificados. Esto resulta particularmente útil para determinar qué atributos se deben especificar en la configuración de la solicitud sin iniciar ninguna instancia. Considere que el comando no tiene en cuenta la capacidad disponible.

Para obtener una vista previa de una lista de tipos de instancias al especificar atributos mediante la AWS CLI

1. (Opcional) Para generar todos los atributos posibles que se pueden especificar, utilice el comando get-instance-types-from-instance-requirements y el parámetro `--generate-cli-skeleton`. Puede dirigir de manera opcional el resultado a un archivo para guardarlo mediante `input > attributes.json`.

   ```
   aws ec2 get-instance-types-from-instance-requirements \
       --region us-east-1 \
       --generate-cli-skeleton input > attributes.json
   ```

   Resultado previsto

   ```
   {
       "DryRun": true,
       "ArchitectureTypes": [
           "i386"
       ],
       "VirtualizationTypes": [
           "hvm"
       ],
       "InstanceRequirements": {
           "VCpuCount": {
               "Min": 0,
               "Max": 0
   ```

```
        },
        "MemoryMiB": {
            "Min": 0,
            "Max": 0
        },
        "CpuManufacturers": [
            "intel"
        ],
        "MemoryGiBPerVCpu": {
            "Min": 0.0,
            "Max": 0.0
        },
        "ExcludedInstanceTypes": [
            ""
        ],
        "InstanceGenerations": [
            "current"
        ],
        "SpotMaxPricePercentageOverLowestPrice": 0,
        "OnDemandMaxPricePercentageOverLowestPrice": 0,
        "BareMetal": "included",
        "BurstablePerformance": "included",
        "RequireHibernateSupport": true,
        "NetworkInterfaceCount": {
            "Min": 0,
            "Max": 0
        },
        "LocalStorage": "included",
        "LocalStorageTypes": [
            "hdd"
        ],
        "TotalLocalStorageGB": {
            "Min": 0.0,
            "Max": 0.0
        },
        "BaselineEbsBandwidthMbps": {
            "Min": 0,
            "Max": 0
        },
        "AcceleratorTypes": [
            "gpu"
        ],
        "AcceleratorCount": {
            "Min": 0,
```

```
            "Max": 0
        },
        "AcceleratorManufacturers": [
            "nvidia"
        ],
        "AcceleratorNames": [
            "a100"
        ],
        "AcceleratorTotalMemoryMiB": {
            "Min": 0,
            "Max": 0
        },
        "NetworkBandwidthGbps": {
            "Min": 0.0,
            "Max": 0.0
        },
        "AllowedInstanceTypes": [
            ""
        ]
    },
    "MaxResults": 0,
    "NextToken": ""
}
```

2. Cree un archivo de configuración JSON con el resultado del paso anterior y configúrelo de la siguiente manera:

> **Note**
>
> Debe proporcionar valores para `ArchitectureTypes`, `VirtualizationTypes`, `VCpuCount` y `MemoryMiB`. Puede omitir los demás atributos; cuando se omiten, se utilizan los valores predeterminados.
> Para obtener una descripción de cada atributo y sus valores predeterminados, consulte get-instance-types-from-instance-requirements en la Referencia de la línea de comandos de Amazon EC2.

a. En `ArchitectureTypes`, especifique uno o varios tipos de arquitectura de procesador.

b. En `VirtualizationTypes`, especifique uno o varios tipos de virtualización.

c. En `VCpuCount`, especifique el número mínimo y máximo de vCPU. Para no especificar un límite mínimo, en `Min`, especifique `0`. Para no especificar un límite máximo, omita el parámetro `Max`.

d. En `MemoryMiB`, especifique la cantidad mínima y máxima de memoria en MiB. Para no especificar un límite mínimo, en `Min`, especifique `0`. Para no especificar un límite máximo, omita el parámetro `Max`.

e. De manera opcional, puede especificar uno o varios de los otros atributos para restringir aún más la lista de tipos de instancias que se devuelven.

3. Para obtener una vista previa de los tipos de instancias que tienen los atributos especificados en el archivo JSON, utilice el comando get-instance-types-from-instance-requirements y especifique el nombre y la ruta de acceso al archivo JSON mediante el parámetro `--cli-input-json`. De manera opcional, puede dar formato al resultado para que aparezca en formato de tabla.

```
aws ec2 get-instance-types-from-instance-requirements \
    --cli-input-json file://attributes.json \
    --output table
```

Archivo de ejemplo *attributes.json*

En este ejemplo, los atributos requeridos se incluyen en el archivo JSON. Ellos son `ArchitectureTypes`, `VirtualizationTypes`, `VCpuCount` y `MemoryMiB`. Además, el atributo opcional `InstanceGenerations` también se incluye. Tenga en cuenta que en `MemoryMiB`, el valor `Max` puede omitirse para indicar que no hay un límite.

```
{
    "ArchitectureTypes": [
        "x86_64"
    ],
    "VirtualizationTypes": [
        "hvm"
    ],
    "InstanceRequirements": {
        "VCpuCount": {
            "Min": 4,
            "Max": 6
        },
        "MemoryMiB": {
            "Min": 2048
        },
```

```
        "InstanceGenerations": [
            "current"
        ]
    }
}
```

Ejemplo de resultado

```
-----------------------------------------
|GetInstanceTypesFromInstanceRequirements|
+---------------------------------------+
||             InstanceTypes             ||
|+-------------------------------------+|
||             InstanceType              ||
|+-------------------------------------+|
||  c4.xlarge                          ||
||  c5.xlarge                          ||
||  c5a.xlarge                         ||
||  c5ad.xlarge                        ||
||  c5d.xlarge                         ||
||  c5n.xlarge                         ||
||  c6a.xlarge                          ||
...
```

4. Después de identificar los tipos de instancia que se ajusten a sus necesidades, anote los atributos de instancia utilizados para poder utilizarlos al configurar su solicitud de flota.

Capacidad bajo demanda en la flota de spot

Para asegurarse de que dispone siempre de capacidad de instancias, puede incluir una solicitud de capacidad bajo demanda en la solicitud de flota de spot. En la solicitud de flota de spot, especifique la capacidad de destino deseada y cuánta debe ser bajo demanda. El saldo incluye la capacidad de spot, que se inicia si hay capacidad de Amazon EC2 disponible y disponibilidad. Por ejemplo, si en la solicitud de flota de spot se especifica 10 como capacidad de destino y 8 como capacidad bajo demanda, Amazon EC2 inicia 8 unidades de capacidad como unidades bajo demanda y 2 unidades de capacidad (10 - 8 = 2) como unidades de spot.

Priorizar tipos de instancias para la capacidad bajo demanda

Cuando la flota de spot intenta cubrir la capacidad bajo demanda, de forma predeterminada inicia primero el tipo de instancia con el precio más bajo. Si `OnDemandAllocationStrategy` se

establece en `prioritized`, la flota de spot aplica la prioridad para determinar qué tipo de instancia debe utilizar primero para cubrir la capacidad bajo demanda.

La prioridad se asigna a la invalidación de la plantilla de lanzamiento y la prioridad más alta se lanza primero.

Ejemplo: priorizar tipos de instancias

En este ejemplo, se configuran tres invalidaciones de plantilla de inicialización, cada una de ellas con un tipo de instancia distinto.

El precio bajo demanda de los tipos de instancias varía. Los siguientes son los tipos de instancias que se utilizan en este ejemplo, presentados por orden de precio, comenzando por el tipo de instancia más barato:

- `m4.large`: la más barata
- `m5.large`
- `m5a.large`

Si no se aplica la prioridad para determinar el orden, la flota cubrirá la capacidad bajo demanda comenzando por el tipo de instancia más barato.

No obstante, supongamos que tiene instancias reservadas `m5.large` sin usar que desea utilizar primero. Puede establecer la prioridad de la invalidación de la plantilla de lanzamiento, de forma que se utilicen los tipos de instancias conforme al orden de prioridad, de la siguiente manera:

- `m5.large`: prioridad 1
- `m4.large`: prioridad 2
- `m5a.large`: prioridad 3

Reequilibrio de la capacidad

Puede configurar la flota de spot para iniciar una instancia de spot de reemplazo cuando Amazon EC2 emita una recomendación de reequilibrio para notificarle que una instancia de spot tiene un riesgo elevado de interrupción. El reequilibrio de la capacidad lo ayuda a mantener la disponibilidad de la carga de trabajo al aumentar de manera proactiva su flota con una nueva instancia de spot antes de que una instancia en ejecución sea interrumpida por Amazon EC2. Para obtener más información, consulte Recomendación de reequilibrio de instancias de EC2.

Para configurar la flota de spot para iniciar una instancia de spot de reemplazo, puede utilizar la consola de Amazon EC2 o la AWS CLI.

- Consola de Amazon EC2: debe seleccionar la casilla de verificación Capacity rebalance (Reequilibrio de capacidad) cuando crea la flota de spot. Para obtener más información, consulte el paso 6.d. en Creación de una solicitud de flota de spot con los parámetros definidos (consola).
- AWS CLI: utilice el comando request-spot-fleet y los parámetros relevantes de la estructura de `SpotMaintenanceStrategies`. Para obtener más información, consulte el ejemplo de configuración de inicio.

Limitaciones

- El reequilibrio de capacidad solo está disponible para flotas de tipo `maintain`.
- Mientras la flota se encuentra en ejecución, no puede modificar la configuración de reequilibrio de capacidad. Para cambiar el ajuste de reequilibrio de capacidad, debe eliminar la flota y crear una nueva.

Opciones de configuración

La `ReplacementStrategy` para la flota de spot admite los siguientes dos valores:

`launch-before-terminate`

Amazon EC2 termina las instancias de spot que reciben una notificación de reequilibrio después de que se lanzan nuevas instancias de spot de reemplazo. Cuando especifica `launch-before-terminate`, también debe especificar un valor para `termination-delay`. Después de que se inician las nuevas instancias de reemplazo, Amazon EC2 espera la duración de `termination-delay` y, luego, termina las instancias antiguas. En `termination-delay`, el mínimo es de 120 segundos (2 minutos) y el máximo es de 7200 segundos (2 horas).

Le recomendamos que utilice `launch-before-terminate` solo si puede predecir cuánto tiempo tardarán en completarse los procedimientos de cierre de instancias. Esto garantizará que las instancias anteriores terminen solo después de que se hayan completado los procedimientos de cierre. Tenga en cuenta que Amazon EC2 puede interrumpir las instancias antiguas con una advertencia de dos minutos antes del `termination-delay`.

`launch`

Amazon EC2 inicia instancias de spot de reemplazo cuando se emite una notificación de reequilibrio para las instancias de spot existentes. Amazon EC2 no termina las instancias que reciben una notificación de reequilibrio. Puede terminar las instancias anteriores o puede dejarlas en ejecución. Se cobrará por todas las instancias mientras se ejecutan.

Consideraciones

Si configura una flota de spot para reequilibrio de la capacidad, tenga en cuenta lo siguiente:

Proporcione tantos grupos de capacidades de spot en la solicitud como sea posible.

Configure su flota de spot para utilizar varios tipos de instancias y zonas de disponibilidad. Esto proporciona la flexibilidad para iniciar instancias de spot en varios grupos de capacidad de spot. Para obtener más información, consulte Sea flexible con respecto a los tipos de instancia y las zonas de disponibilidad.

Evite un riesgo elevado de interrupción de instancias de spot de reemplazo

Para evitar un alto riesgo de interrupción, recomendamos la estrategia de asignación de `capacityOptimized` o `capacityOptimizedPrioritized`. Estas estrategias garantizan que las instancias de spot de reemplazo se inicien en los grupos de capacidad de spot más óptimos; por lo tanto, es menos probable que se interrumpan en un futuro cercano. Para obtener más información, consulte Utilice la estrategia de asignación optimizada para capacidad y precio.

Amazon EC2 solo iniciará una nueva instancia si la disponibilidad es la misma o superior

Uno de los objetivos del reequilibrio de la capacidad es mejorar la disponibilidad de una instancia de spot. Si una instancia de spot existente recibe una recomendación de reequilibrio, Amazon EC2 solo iniciará una nueva instancia si esta ofrece la misma disponibilidad o una mejor que la instancia existente. Si el riesgo de interrupción de una nueva instancia es peor que el de la instancia existente, Amazon EC2 no iniciará ninguna instancia nueva. Sin embargo, Amazon EC2 seguirá evaluando los grupos de capacidad de spot e iniciará una nueva instancia si la disponibilidad mejora.

Existe la posibilidad de que la instancia existente se interrumpa sin que Amazon EC2 lance una nueva instancia de forma proactiva. Cuando esto ocurre, Amazon EC2 intentará iniciar una nueva instancia, independientemente de si la nueva instancia tiene un alto riesgo de interrupción.

El reequilibrio de la capacidad no aumenta la tasa de interrupciones de las instancias de spot

Cuando habilita el reequilibrio de capacidad, no aumenta la tasa de interrupciones de las instancias de spot (el número de instancias de spot que se reclaman cuando Amazon EC2 necesita recuperar la capacidad). Sin embargo, si el reequilibrio de capacidad detecta que una instancia está en riesgo de interrupción, Amazon EC2 intentará iniciar inmediatamente una nueva instancia. El resultado es que se pueden reemplazar más instancias en lugar de esperar a que Amazon EC2 lance una nueva después de que se interrumpa la instancia en riesgo.

Si bien es posible que se reemplacen más instancias con el reequilibrio de capacidad habilitado, se beneficia de ser proactivo en lugar de reactivo al disponer de más tiempo para tomar medidas antes de que se interrumpan las instancias. Con un aviso de interrupción de instancias de spot, normalmente solo dispone de dos minutos para apagar correctamente la instancia. Con el reequilibrio de capacidad que inicia una nueva instancia por adelantado, le da a los procesos existentes una mejor oportunidad de completarse en la instancia en riesgo, puede iniciar los procedimientos de apagado de la instancia y evitar que se programen nuevos trabajos en la instancia en riesgo. También puede empezar a preparar la instancia recién iniciada para que se haga cargo de la aplicación. Con el reemplazo proactivo del reequilibrio de capacidad, se beneficia de una continuidad estable.

Como ejemplo teórico para demostrar los riesgos y beneficios del uso del reequilibrio de capacidad, considere el siguiente escenario:

- 14:00 h: se recibe una recomendación de reequilibrio para la instancia A y Amazon EC2 comienza inmediatamente a intentar iniciar una instancia B de reemplazo, lo que le da tiempo para iniciar los procedimientos de apagado.*
- 14:30 h: se recibe una recomendación de reequilibrio para la instancia B, sustituida por la instancia C, lo que le da tiempo para iniciar los procedimientos de apagado.*
- 14:32 h: si el reequilibrio de capacidad no estuviera habilitado y si se hubiera recibido un aviso de interrupción de la instancia de spot a las 14:32 para la instancia A, solo habría tenido hasta dos minutos para actuar, pero la instancia A habría estado funcionando hasta ese momento.

* Si se especifica `launch-before-terminate`, Amazon EC2 terminará la instancia en riesgo después de que se conecte la instancia de reemplazo.

Amazon EC2 puede lanzar nuevas instancias de spot de reemplazo hasta que la capacidad utilizada sea el doble de la capacidad de destino

Cuando una flota de spot se configura para reequilibrio de la capacidad, Amazon EC2 intenta iniciar una nueva instancia de spot de reemplazo para cada instancia de spot que recibe una

recomendación de reequilibrio. Después de que una instancia de spot reciba una recomendación de reequilibrio, ya no se cuenta como parte de la capacidad cumplida. Según la estrategia de reemplazo, Amazon EC2 termina la instancia después de un retraso de terminación preconfigurado o la deja en ejecución. Esto le da la oportunidad de realizar acciones de reequilibrio en la instancia.

Si su flota alcanza el doble de su capacidad de destino, deja de iniciar nuevas instancias de reemplazo, incluso si las propias instancias de reemplazo reciben una recomendación de reequilibrio.

Por ejemplo, puede crear una flota de spot con una capacidad de destino de 100 instancias de spot. Todas las instancias de spot reciben una recomendación de reequilibrio, que provoca que Amazon EC2 lance 100 instancias de spot de reemplazo. Esto eleva el número de instancias de spot utilizadas a 200, lo que es el doble de la capacidad de destino. Algunas de las instancias de reemplazo reciben una recomendación de reequilibrio, pero no se inician más instancias de reemplazo porque la flota no puede exceder el doble de su capacidad objetivo.

Tenga en cuenta que se le cobrarán todas las instancias mientras se ejecutan.

Le recomendamos que configure la flota de spot para que termine las instancias de spot que reciban una recomendación de reequilibrio

Si configura su flota de spot para el reequilibrio de la capacidad, recomendamos que elija `launch-before-terminate` con un retraso de terminación adecuado solo si puede predecir cuánto tardarán en completarse los procedimientos de cierre de la instancia. Esto garantizará que las instancias anteriores terminen solo después de que se hayan completado los procedimientos de cierre.

Si elige terminar las instancias recomendadas para reequilibrio, le recomendamos que monitoree la señal de recomendación de reequilibrio recibida por las instancias de spot de la flota. Mediante la supervisión de la señal, puede realizar rápidamente acciones de reequilibrio en las instancias afectadas antes de que Amazon EC2 las interrumpa y luego puede finalizarlas manualmente. Si no termina las instancias, continuará pagándolas mientras se ejecuten. Amazon EC2 no termina automáticamente las instancias que reciben una recomendación de reequilibrio.

Puede configurar notificaciones mediante Amazon EventBridge o metadatos de instancia. Para obtener más información, consulte Monitorear las señales de recomendación de reequilibrio.

La flota de spot no cuenta las instancias que reciben una recomendación de reequilibrio cuando se calcula la capacidad utilizada durante la reducción o el escalado horizontal

Si la flota de spot está configurada para reequilibrio de la capacidad y cambia la capacidad de destino, ya sea para la reducción horizontal o el escalado horizontal, la flota no cuenta las instancias marcadas para el reequilibrio como parte de la capacidad utilizada, de la siguiente manera:

- Reducción horizontal: si reduce la capacidad de destino deseada, Amazon EC2 termina las instancias que no están marcadas para reequilibrar hasta que se alcance la capacidad deseada. Las instancias marcadas para el reequilibrio no se cuentan para la capacidad utilizada.

  Por ejemplo, puede crear una flota de spot con una capacidad de destino de 100 instancias de spot. 10 instancias reciben una recomendación de reequilibrio, por lo que Amazon EC2 inicia 10 nuevas instancias de reemplazo, lo que da como resultado una capacidad utilizada de 110 instancias. A continuación, se reduce la capacidad de destino a 50 (reducción horizontal), pero la capacidad utilizada es en realidad de 60 instancias porque Amazon EC2 no termina las 10 instancias marcadas para el reequilibrio. Debe terminar manualmente estas instancias o puede dejarlas en ejecución.
- Escalado horizontal: si aumenta la capacidad de destino deseada, Amazon EC2 lanza nuevas instancias hasta que se alcance la capacidad deseada. Las instancias marcadas para el reequilibrio no se cuentan para la capacidad utilizada.

  Por ejemplo, puede crear una flota de spot con una capacidad de destino de 100 instancias de spot. 10 instancias reciben una recomendación de reequilibrio, por lo que Amazon EC2 lanza 10 nuevas instancias de reemplazo, lo que da como resultado una capacidad utilizada de 110 instancias. A continuación, aumenta la capacidad de destino a 200 (escalado ascendente), pero la capacidad utilizada es en realidad 210 instancias porque las 10 instancias marcadas para el reequilibrio no son contadas por la flota como parte de la capacidad de destino. Debe terminar manualmente estas instancias o puede dejarlas en ejecución.

Anulaciones de precios de spot

Cada solicitud de flota de spot puede incluir un precio máximo global o usar el predeterminado (el precio bajo demanda). La flota de spot usa este precio como el máximo predeterminado para cada una de sus especificaciones de inicialización.

Si lo desea, puede especificar un precio máximo en una o más especificaciones de lanzamiento. Este precio es específico de la especificación de lanzamiento. Si una especificación de inicialización incluye un precio específico, la flota de spot usa este precio máximo para invalidar el global. Cualquier otra especificación de lanzamiento que no incluya un precio máximo específico seguirá usando el precio máximo global.

Control de gastos

La flota de spot deja de iniciar instancias cuando se alcanza la capacidad de destino o la cantidad máxima que está dispuesto a pagar. Para controlar la cantidad que paga por hora por su flota, puede especificar el `SpotMaxTotalPrice` por instancias de spot y el `OnDemandMaxTotalPrice` por instancias bajo demanda. Cuando se alcanza el precio máximo total, la flota de spot deja de iniciar instancias, incluso si no se ha alcanzado la capacidad de destino.

En los siguientes ejemplos, se muestran dos situaciones diferentes. En el primero, la flota de spot deja de iniciar instancias cuando se alcanza la capacidad de destino. En el segundo, la flota de spot deja de iniciar instancias cuando se alcanza la cantidad máxima que está dispuesto a pagar.

Ejemplo: dejar de lanzar instancias cuando se alcanza la capacidad de destino

Dada una solicitud de Instancias bajo demanda`m4.large`, donde:

- Precio bajo demanda: 0,10 USD por hora
- `OnDemandTargetCapacity`: 10
- `OnDemandMaxTotalPrice`: 1,50 USD

La flota de spot inicia 10 instancias bajo demanda porque el total de 1,00 USD (10 instancias x 0,10 USD) no supera el `OnDemandMaxTotalPrice` de 1,50 USD.

Ejemplo: dejar de lanzar instancias cuando se alcanza el precio máximo total

Dada una solicitud de Instancias bajo demanda`m4.large`, donde:

- Precio bajo demanda: 0,10 USD por hora
- `OnDemandTargetCapacity`: 10
- `OnDemandMaxTotalPrice`: 0,80 USD

Si la flota de spot inicia la capacidad de destino bajo demanda (10 instancias bajo demanda), el costo total por hora sería de 1,00 USD. Esto es más que la cantidad especificada (0,80 USD) como

`OnDemandMaxTotalPrice`. Para evitar gastar más de lo que está dispuesto a pagar, la flota de spot inicia solo 8 instancias bajo demanda (por debajo de la capacidad de destino bajo demanda) porque iniciar más superaría el `OnDemandMaxTotalPrice`.

Ponderación de instancias de flota de spot

Cuando se solicita una flota de instancias de spot, se pueden definir las unidades de capacidad con las que cada tipo de instancia contribuye al rendimiento de la aplicación y ajustar el precio máximo de cada grupo según corresponda mediante la ponderación de instancias.

De forma predeterminada, el precio se especifica por hora de instancia. Cuando se utiliza la característica de ponderación de instancias, el precio se especifica por hora de unidad. Puede calcular el precio por hora de unidad mediante la división del precio de un tipo de instancia por el número de unidades que representa. La flota de spot calcula el número de instancias de spot que debe iniciar mediante la división de la capacidad de destino por la ponderación de instancias. Si el resultado no es un entero, la flota de spot lo redondea al siguiente entero, de manera que el tamaño de la flota no esté por debajo de su capacidad de destino. La flota de spot puede seleccionar cualquier grupo que indique en la especificación de inicialización, incluso si la capacidad de las instancias iniciadas sobrepasa la capacidad de destino solicitada.

En las siguientes tablas se incluyen ejemplos de cálculos para determinar el precio por unidad para una solicitud de flota de spot con una capacidad de destino de 10.

Tipo de instancia	Ponderación de instancia	Precio por hora de instancia	Precio por hora de unidad	Número de instancias lanzadas
`r3.xlarge`	2	0,05 USD	0,025 (0,05 dividido por 2)	5 (10 dividido por 2)

Tipo de instancia	Ponderación de instancia	Precio por hora de instancia	Precio por hora de unidad	Número de instancias lanzadas
`r3.8xlarge`	8	0,10 USD	0,0125 (0,10 dividido por 8)	2 (10 dividido por 8, con el resultado redondeado hacia arriba)

Use la ponderación de instancias de flota de spot de la siguiente manera para aprovisionar la capacidad de destino que desea en los grupos con el precio más bajo por unidad en el momento de su tramitación:

1. Establezca la capacidad de destino de la flota de spot en instancias (opción predeterminada) o en las unidades de su elección, como CPU virtuales, memoria, almacenamiento o rendimiento.
2. Establezca el precio por unidad.
3. Para cada configuración de inicialización, especifique la ponderación, que es el número de unidades con el que el tipo de instancia representa la capacidad de destino.

Ejemplo de ponderación de instancias

Considere una solicitud de flota de spot con la siguiente configuración:

- Una capacidad de destino de 24
- Una especificación de inicialización con un tipo de instancia `r3.2xlarge` y una ponderación de 6
- Una especificación de inicialización con un tipo de instancia `c3.xlarge` y una ponderación de 5

La ponderación representa el número de unidades con el que el tipo de instancia representa la capacidad de destino. Si la primera especificación de inicialización proporciona el precio por unidad más bajo (precio para `r3.2xlarge` por hora de instancia dividido entre 6), la flota de spot debería iniciar 4 de estas instancias (24 dividido entre 6).

Si la segunda especificación de inicialización proporciona el precio por unidad más bajo (precio para `c3.xlarge` por hora de instancia dividido por 5), la flota de spot debería iniciar 5 de estas instancias (24 dividido por 5, con el resultado redondeado hacia arriba).

Ponderación de instancias y estrategia de asignación

Considere una solicitud de flota de spot con la siguiente configuración:

- Una capacidad de destino de 30
- Una especificación de lanzamiento con un tipo de instancia `c3.2xlarge` y una ponderación de 8
- Una especificación de lanzamiento con un tipo de instancia `m3.xlarge` y una ponderación de 8
- Una especificación de lanzamiento con un tipo de instancia `r3.xlarge` y una ponderación de 8

La flota de spot debería iniciar cuatro instancias (30 dividido por 8, con el resultado redondeado hacia arriba). Con la estrategia `diversified`, la flota de spot inicia una instancia en cada uno de los tres grupos y la cuarta instancia en cualquiera de los grupos que proporcione el menor precio por unidad.

Trabajar con flotas de spot

A fin de comenzar a utilizar una flota de spot, cree una solicitud de flota de spot que incluya la capacidad de destino, una parte opcional bajo demanda, una o varias especificaciones de inicialización para las instancias y el precio máximo que está dispuesto a pagar. La solicitud de flota deberá incluir una especificación de inicialización que defina la información que la flota requiere para iniciar una instancia, como una AMI, un tipo de instancias, una subred o una zona de disponibilidad y uno o varios grupos de seguridad.

Si la flota incluye Instancias de spot, Amazon EC2 puede intentar mantener la capacidad de destino de la flota cuando los precios de spot cambien.

Una vez que se ha enviado la solicitud, no es posible modificar la capacidad de destino de una solicitud puntual. Para cambiar la capacidad de destino, cancelar la solicitud y enviar una nueva.

Una solicitud de flota de spot permanece activa hasta que vence o hasta que usted la cancela. Cuando cancela una solicitud de flota, puede especificar si se terminan las instancias de spot de esa flota con la cancelación de la solicitud.

Contenido

Estados de una solicitud de flota de spot

Una solicitud de flota de spot puede tener uno de los siguientes estados:

- `submitted`: se evalúa la solicitud de la flota de spot y Amazon EC2 se prepara para iniciar el número objetivo de instancias. Si una solicitud excede los límites de la flota de spot, se cancela inmediatamente.
- `active`: la flota de spot se validó y Amazon EC2 intenta mantener el número objetivo de instancias de spot en ejecución. La solicitud permanece en este estado hasta que se modifica o se cancela.
- `modifying`: se modifica la solicitud de la flota de spot. La solicitud permanece en este estado hasta que la modificación se procese completamente o se cancele la flota de spot. Una solicitud (`request`) de una única vez no se puede modificar y este estado no se aplica a estas solicitudes de spot.
- `cancelled_running`: la flota de spot se cancela y no inicia instancias de spot adicionales. Las instancias de spot existentes continúan ejecutándose hasta que se interrumpen o terminan. La solicitud permanece en este estado hasta que se interrumpan o terminen todas las instancias.
- `cancelled_terminating`: la flota de spot se cancela y sus instancias de spot terminan. La solicitud permanece en este estado hasta que se terminen todas las instancias.
- `cancelled`: la flota de spot se cancela y no tiene instancias de spot en ejecución. La solicitud de flota de spot se elimina dos días después de la terminación de sus instancias.

Comprobaciones de estado de la flota de spot

La flota de spot verifica el estado de las instancias de spot de la flota cada dos minutos. El estado de una instancia puede ser `healthy` o `unhealthy`.

La flota de spot determina el estado de una instancia a partir de las verificaciones de estado que proporciona Amazon EC2. Una instancia se determina como `unhealthy` cuando el estado de la comprobación del estado de la instancia o de la comprobación del estado del sistema es `impaired` durante tres comprobaciones de estado consecutivas. Para obtener más información, consulte Comprobaciones de estado para sus instancias.

Puede configurar la flota para sustituir la Instancias de spot en mal estado. Después de habilitar el reemplazo de la comprobación de estado, se reemplaza una instancia de spot cuando se notifica como `unhealthy`. La flota podría ver reducida su capacidad de destino durante algunos minutos mientras se reemplaza una instancia de spot en mal estado.

Requisitos

- El reemplazo por comprobación de estado se admite solo para que Flotas de spot mantenga una capacidad de destino (flotas de tipo `maintain`), no para Flotas de spot puntual (flotas de tipo `request`).
- Solo se admite el reemplazo por comprobación de estado para Instancias de spot. Esta función no es compatible con Instancias bajo demanda.
- Solo puede configurar una flota de spot para reemplazar instancias en mal estado al momento de crearla.
- Los usuarios pueden utilizar el reemplazo por comprobación de estado únicamente si tienen permiso para llamar a la acción `ec2:DescribeInstanceStatus`.

Console

Para configurar una flota de spot que sustituya instancias de spot en mal estado mediante la consola

1. Siga los pasos para crear una flota de spot. Para obtener más información, consulte Creación de una solicitud de flota de spot con los parámetros definidos (consola).
2. Para configurar la flota que sustituya las instancias de spot en mal estado, en Comprobación de estado, seleccione Sustituir instancias en mal estado. Para habilitar esta opción, primero debe elegir Mantener capacidad de destino.

AWS CLI

Para configurar una flota de spot que sustituya instancias de spot en mal estado mediante la AWS CLI

1. Siga los pasos para crear una flota de spot. Para obtener más información, consulte Creación de una flota de spot mediante la AWS CLI.
2. Para configurar la flota que sustituya la instancias de spot en mal estado, para `ReplaceUnhealthyInstances`, escriba `true`.

Permisos de flota de spot

Si los usuarios van a crear o administrar una flota de spot, tiene que concederles los permisos necesarios.

Si utiliza la consola de Amazon EC2 para crear una flota de spot, se crean dos roles vinculados a servicios denominados `AWSServiceRoleForEC2SpotFleet` y `AWSServiceRoleForEC2Spot` y un rol denominado `aws-ec2-spot-fleet-tagging-role` que otorgan a la flota de spot los permisos para solicitar, iniciar, terminar y etiquetar recursos en su nombre. Si utiliza la AWS CLI o una API, debe asegurarse de que existen estos roles.

Siga las instrucciones siguientes para conceder los permisos necesarios y crear los roles.

Permisos y roles

- Concesión de permisos a los usuarios para la flota de spot
- Rol vinculado a servicios de flota de spot
- Rol vinculado a un servicio para instancias de spot
- Rol de IAM para etiquetar una flota de spot

Concesión de permisos a los usuarios para la flota de spot

Si los usuarios van a crear o administrar una flota de spot, asegúrese de concederles los permisos necesarios.

Para crear una política para la flota de spot

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.

2. En el panel de navegación, seleccione Policies (Políticas), Create policy (Crear política).
3. En la página Crear política elija JSON y reemplace el texto por el siguiente.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances",
                "ec2:CreateTags",
                "ec2:RequestSpotFleet",
                "ec2:ModifySpotFleetRequest",
                "ec2:CancelSpotFleetRequests",
                "ec2:DescribeSpotFleetRequests",
                "ec2:DescribeSpotFleetInstances",
                "ec2:DescribeSpotFleetRequestHistory"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::*:role/aws-ec2-spot-fleet-tagging-role"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole",
                "iam:ListRoles",
                "iam:ListInstanceProfiles"
            ],
            "Resource": "*"
        }
    ]
}
```

La política de ejemplo anterior concede a un usuario los permisos necesarios para la mayoría de los casos de uso de la flota de spot. Para limitar las acciones del usuario a unas determinadas acciones de la API, especifique dichas acciones de la API en su lugar.

API de IAM y EC2 requeridas

Las siguientes API deben incluirse en la política:

- `ec2:RunInstances`: se necesita para iniciar instancias en una flota de spot
- `ec2:CreateTags`: se necesita para etiquetar la solicitud, las instancias o los volúmenes de la flota de spot
- `iam:PassRole`: se necesita para especificar el rol de la flota de spot
- `iam:CreateServiceLinkedRole`: se necesita para crear el rol vinculado a servicios
- `iam:ListRoles`: se necesita para enumerar los roles de IAM existentes
- `iam:ListInstanceProfiles`: se necesita para enumerar los perfiles de instancia existentes

> **Important**
>
> Si especifica un rol para el perfil de instancia de IAM en la especificación de inicialización o en la plantilla de inicialización, debe conceder al usuario el permiso para pasar el rol al servicio. Para ello, incluya "`arn:aws:iam::*:role/`*`IamInstanceProfile-role`*" como recurso en la política de IAM para la acción `iam:PassRole`. Para obtener más información, consulte Concesión de permisos a un usuario para transferir un rol a un servicio de AWS en la Guía del usuario de IAM.

API de flota de spot

Agregue las siguientes acciones de API de flota de spot a su política, según sea necesario:

- `ec2:RequestSpotFleet`
- `ec2:ModifySpotFleetRequest`
- `ec2:CancelSpotFleetRequests`
- `ec2:DescribeSpotFleetRequests`
- `ec2:DescribeSpotFleetInstances`
- `ec2:DescribeSpotFleetRequestHistory`

API de IAM opcionales

(Opcional) Para permitir a un usuario crear roles o perfiles de instancia mediante la consola de IAM, debe agregar las siguientes acciones a la política:

- `iam:AddRoleToInstanceProfile`
- `iam:AttachRolePolicy`
- `iam:CreateInstanceProfile`
- `iam:CreateRole`
- `iam:GetRole`
- `iam:ListPolicies`

4. Elija Review policy.
5. En la página Revisar política, escriba un nombre y descripción de política y, a continuación, elija Crear política.
6. Para dar acceso, agregue permisos a los usuarios, grupos o roles:

   - Usuarios y grupos en AWS IAM Identity Center:

     Cree un conjunto de permisos. Siga las instrucciones de Creación de un conjunto de permisos en la Guía del usuario de AWS IAM Identity Center.

   - Usuarios administrados en IAM a través de un proveedor de identidades:

     Cree un rol para la federación de identidades. Siga las instrucciones descritas en Creación de un rol para un proveedor de identidad de terceros (federación) en la Guía del usuario de IAM.

   - Usuarios de IAM:
     - Cree un rol que el usuario pueda aceptar. Siga las instrucciones descritas en Creación de un rol para un usuario de IAM en la Guía del usuario de IAM.
     - (No recomendado) Adjunte una política directamente a un usuario o añada un usuario a un grupo de usuarios. Siga las instrucciones descritas en Adición de permisos a un usuario (consola) de la Guía del usuario de IAM.

Rol vinculado a servicios de flota de spot

Amazon EC2 utiliza roles vinculados a un servicio para los permisos que necesita para llamar a otros servicios de AWS en su nombre. Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a un servicio de AWS. Los roles vinculados a servicios ofrecen una manera segura de delegar permisos a los servicios de AWS, ya que solo los servicios vinculados

pueden asumir roles vinculados a servicios. Para obtener más información, consulte Uso de roles vinculados a servicios en la Guía del usuario de IAM.

Amazon EC2 usa el rol vinculado a un servicio denominado AWSServiceRoleForEC2SpotFleet para iniciar y administrar instancias en su nombre.

> **Important**
>
> Si especifica una AMI cifrada o una instantánea de Amazon EBS cifrada en su flota de spot, debe conceder permiso al rol AWSServiceRoleForEC2SpotFleet para utilizar la CMK a fin de que Amazon EC2 pueda iniciar instancias en su nombre. Para obtener más información, consulte Conceder acceso a CMK para su uso con AMI cifradas e instantáneas de EBS.

Permisos concedidos por AWSServiceRoleForEC2SpotFleet

Amazon EC2 usa AWSServiceRoleForEC2SpotFleet para completar las acciones siguientes:

- `ec2:RequestSpotInstances`: solicitar instancias de spot
- `ec2:RunInstances`: para iniciar las instancias
- `ec2:TerminateInstances`: para terminar las instancias
- `ec2:DescribeImages`: para describir imágenes de Amazon Machine (AMI) para las instancias
- `ec2:DescribeInstanceStatus`: para describir el estado de las instancias
- `ec2:DescribeSubnets`: describen las subredes de las instancias
- `ec2:CreateTags`: agrega etiquetas a la solicitud, las instancias y los volúmenes de la flota de spot
- `elasticloadbalancing:RegisterInstancesWithLoadBalancer`: para agregar las instancias especificadas al equilibrador de carga especificado
- `elasticloadbalancing:RegisterTargets`: para registrar los destinos especificados con el grupo de destino especificado

Creación del rol vinculado a servicio

En la mayoría de los casos, no es necesario crear manualmente roles vinculados a servicios. Amazon EC2 crea el rol vinculado a un servicio AWSServiceRoleForEC2SpotFleet la primera vez que se crea una flota de spot con la consola.

Si tenía una solicitud de flota de spot activa antes de octubre de 2017, cuando Amazon EC2 comenzó a respaldar este rol vinculado a un servicio, Amazon EC2 creó el rol AWSServiceRoleForEC2SpotFleet en su cuenta de AWS. Para obtener más información, consulte Un nuevo rol ha aparecido en la cuenta de AWS en la Guía del usuario de IAM.

Si utiliza la AWS CLI o una API para crear una flota de spot, primero debe asegurarse de que este rol existe.

Para crear AWSServiceRoleForEC2SpotFleet mediante la consola

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. Seleccione Roles en el panel de navegación.
3. Elija Crear rol.
4. En la página Seleccionar entidad de confianza, haga lo siguiente:
   a. En Tipo de entidad de confianza, elija Servicio de AWS.
   b. En la sección Caso de uso, en Servicio o caso de uso, elija EC2.
   c. En Caso de uso, elija EC2 - Flota de spot.
   d. Elija Siguiente.
5. En la página Agregar permisos, elija Siguiente.
6. En la página Nombrar, revisar y crear, elija Crear rol.

Para crear AWSServiceRoleForEC2SpotFleet mediante el comando AWS CLI

Utilice el comando create-service-linked-role de la siguiente manera.

```
aws iam create-service-linked-role --aws-service-name spotfleet.amazonaws.com
```

Si ya no tiene que utilizar la flota de spot, le recomendamos que elimine el rol AWSServiceRoleForEC2SpotFleet. Después de eliminar este rol de su cuenta, Amazon EC2 volverá a crearlo si solicita una flota de spot mediante la consola. Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Conceder acceso a CMK para su uso con AMI cifradas e instantáneas de EBS

Si especifica una AMI cifrada o una instantánea de Amazon EBS cifrada en su solicitud de flota de spot y usa una clave administrada por el cliente para el cifrado, debe conceder permiso al rol

AWSServiceRoleForEC2SpotFleet para que use la CMK a fin de que Amazon EC2 pueda iniciar instancias en su nombre. Para ello, debe añadir una concesión a la CMK, como se muestra en el siguiente procedimiento.

Al proporcionar permisos, las concesiones son una alternativa a las políticas de claves. Para obtener más información, consulte Uso de concesiones y Uso de políticas de claves en AWS KMS en la Guía para desarrolladores de AWS Key Management Service.

Para conceder permisos al rol AWSServiceRoleForEC2SpotFleet para que use la CMK

- Use el comando create-grant para añadir una concesión a la CMK y para especificar la entidad principal (el rol vinculado a un servicio AWSServiceRoleForEC2SpotFleet) que recibe permiso para realizar las operaciones que permite la concesión.cin La CMK se especifica con el parámetro `key-id` y el ARN de la CMK. La entidad principal se especifica con el parámetro `grantee-principal` y el ARN del rol vinculado a un servicio AWSServiceRoleForEC2SpotFleet.

```
aws kms create-grant \
    --region us-east-1 \
    --key-id arn:aws:kms:us-
east-1:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:role/
AWSServiceRoleForEC2SpotFleet \
    --operations "Decrypt" "Encrypt" "GenerateDataKey"
 "GenerateDataKeyWithoutPlaintext" "CreateGrant" "DescribeKey" "ReEncryptFrom"
 "ReEncryptTo"
```

Rol vinculado a un servicio para instancias de spot

Amazon EC2 usa el rol vinculado a un servicio denominado AWSServiceRoleForEC2Spot para iniciar y administrar instancias de spot en su nombre. Para obtener más información, consulte Rol vinculado al servicio para solicitudes de instancias de spot.

Rol de IAM para etiquetar una flota de spot

El rol de IAM `aws-ec2-spot-fleet-tagging-role` concede el permiso de flota de spot para etiquetar la solicitud, las instancias y los volúmenes de la flota de spot. Para obtener más información, consulte Etiquetado de una flota de spot.

> **Important**
>
> Si decide etiquetar las instancias de la flota y mantener la capacidad de destino (la solicitud de flota de spot es de tipo `maintain`), las diferencias de los permisos que se configuran para el usuario e `IamFleetRole` pueden provocar un comportamiento de etiquetado incoherente de las instancias de la flota. Si el `IamFleetRole` no incluye el permiso `CreateTags`, es posible que algunas de las instancias iniciadas por la flota no estén etiquetadas. Mientras trabajamos para corregir esta incoherencia, para asegurarnos de que todas las instancias iniciadas por la flota estén etiquetadas, recomendamos que utilice el rol `aws-ec2-spot-fleet-tagging-role` para el `IamFleetRole`. Como alternativa, para utilizar un rol existente, asocie la política administrada `AmazonEC2SpotFleetTaggingRole` de AWS al rol existente. De lo contrario, debe agregar manualmente el permiso `CreateTags` a la política existente.

Para crear el rol de IAM para etiquetar una flota de spot

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. Seleccione Roles en el panel de navegación.
3. Elija Crear rol.
4. En la página Seleccionar entidad de confianza, en Tipo de entidad de confianza, elija Servicio de AWS.
5. En Caso de uso, en Casos de uso para otros servicios de AWS, elija EC2 y, a continuación, EC2: etiquetado de flota de spot.
6. Elija Siguiente.
7. En la página Agregar permisos, elija Siguiente.
8. En la página Name, review, and create (Nombrar, revisar y crear), en Role name (Nombre del rol), ingrese un nombre para el rol (por ejemplo, **`aws-ec2-spot-fleet-tagging-role`**).
9. Revise la información de la página, y luego elija Create role (Crear rol).

Prevención de la sustitución confusa entre servicios

El problema de la sustitución confusa es un problema de seguridad en el que una entidad que no tiene permiso para realizar una acción puede obligar a una entidad con más privilegios a realizar la acción. Se recomienda utilizar las claves de contexto de condición global `aws:SourceArn` y

aws:SourceAccount en la política de confianza aws-ec2-spot-fleet-tagging-role con el fin de limitar los permisos que la flota de spot concede a otro servicio para el recurso.

Para agregar las claves de condición aws:SourceArn y aws:SourceAccount a la política de confianza **aws-ec2-spot-fleet-tagging-role**

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. Seleccione Roles en el panel de navegación.
3. Busque la aws-ec2-spot-fleet-tagging-role que haya creado anteriormente y elija el enlace (no la casilla de verificación).
4. En Resumen, elija la pestaña Relaciones de confianza, y luego Editar política de confianza.
5. En la instrucción JSON, agregue un elemento Condition que contenga las claves de contexto de condición global aws:SourceAccount y aws:SourceArn para evitar el problema del suplente confuso de la siguiente manera:

```
"Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:ec2:us-east-1:account_id:spot-fleet-request/sfr-
*"
      },
      "StringEquals": {
        "aws:SourceAccount": "account_id"
      }
```

> **Note**
>
> Si el valor aws:SourceArn contiene el ID de la cuenta y utiliza ambas claves de contexto de condición global, el valor aws:SourceAccount y la cuenta del valor aws:SourceArn deben utilizar el mismo ID de cuenta cuando se empleen en la misma instrucción de política.

La política de confianza final será como sigue:

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
```

```
    "Effect": "Allow",
    "Principal": {
      "Service": "spotfleet.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:ec2:us-east-1:account_id:spot-fleet-request/sfr-
*"
      },
      "StringEquals": {
        "aws:SourceAccount": "account_id"
      }
    }
  }
}
```

6. Elija Actualizar política.

La siguiente tabla proporciona los valores potenciales de `aws:SourceArn` para limitar el alcance de `aws-ec2-spot-fleet-tagging-role` en distintos grados de especificidad.

Operación de la API	Servicio llamado	Ámbito	**aws:SourceArn**
RequestSpotFleet	AWS STS (AssumeRole)	Limite la capacidad de AssumeRole en aws-ec2-spot-fleet-tagging-role a las solicitudes de flota de spot en la cuenta especificada.	arn:aws:ec2:*: *123456789012* :spot-fleet-request/sfr-*
RequestSpotFleet	AWS STS (AssumeRole)	Limite la capacidad de AssumeRole en aws-ec2-spot-fleet-tagging-role a las solicitudes de flota de spot en la cuenta especific	arn:aws:ec2: *us-east-1* :*123456789012* :spot-fleet-request/sfr-*

Operación de la API	Servicio llamado	Ámbito	**aws:SourceArn**
		ada y en la región especificada. Tenga en cuenta que este rol no se podrá utilizar en otras regiones.	
RequestSpotFleet	AWS STS (`AssumeRole`)	Limite la capacidad de `AssumeRole` en `aws-ec2-spot-fleet-tagging-role` solo a las acciones que afecten a la flota sfr-11111111-1111-1111-1111-111111111111. Tenga en cuenta que es posible que este rol no se pueda utilizar para otras flotas de spot. Además, este rol no se puede utilizar para iniciar ninguna nueva flota de spot a través de request-spot-fleet.	`arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-11111111-1111-1111-1111-111111111111`

Creación de una solicitud de flota de spot

Desde la AWS Management Console, cree rápidamente una solicitud de flota de spot mediante la selección de la aplicación o la tarea que necesita y las especificaciones de computación mínimas. Amazon EC2 configura una flota que mejor se ajuste a sus necesidades y sigue la práctica recomendada de spot. Para obtener más información, consulte Creación rápida de una solicitud de flota de spot (consola). De lo contrario, puede modificar la configuración predeterminada. Para obtener más información, consulte Creación de una solicitud de flota de spot con los parámetros definidos (consola) y Creación de una flota de spot mediante la AWS CLI.

Opciones para crear una flota de spot

- Creación rápida de una solicitud de flota de spot (consola)
- Creación de una solicitud de flota de spot con los parámetros definidos (consola)
- Creación de una flota de spot mediante la AWS CLI

Creación rápida de una solicitud de flota de spot (consola)

Para crear una solicitud de flota de spot rápidamente, siga estos pasos.

Para crear una solicitud de flota de spot con la configuración recomendada (consola)

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Solicitudes de spot.
3. Si es la primera vez que utiliza instancias de spot, aparecerá una página de bienvenida; elija Comenzar. De lo contrario, elija Solicitar instancias de spot.
4. En Parámetros de inicialización, elija Configurar los parámetros de inicialización de forma manual.
5. En AMI, elija una AMI.
6. En Capacidad de destino, para Capacidad total de destino, especifique el número de unidades que desea solicitar. Para el tipo de unidad, puede elegir Instances (Instancias), vCPU o Memory (MiB) (Memoria [MiB]).
7. En Su solicitud de flota de un vistazo, revise la configuración de la flota y elija Inicialización.

Creación de una solicitud de flota de spot con los parámetros definidos (consola)

Puede crear una flota de spot con los parámetros que defina.

Para crear una solicitud de flota de spot con los parámetros definidos (consola)

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Solicitudes de spot.
3. Si es la primera vez que utiliza instancias de spot, aparecerá una página de bienvenida; elija Comenzar. De lo contrario, elija Solicitar instancias de spot.
4. En Parámetros de inicialización, haga lo siguiente:

a. Para definir los parámetros de inicialización en la consola de spot, elija Configurar los parámetros de inicialización de forma manual.

b. En AMI, elija una de las AMI básicas que proporciona AWS, o bien elija Buscar AMI para utilizar una AMI de nuestra comunidad de usuarios, del AWS Marketplace o una suya propia.

> **Note**
>
> Si se anula o inhabilita una AMI especificada en los parámetros de inicialización, no se podrán iniciar nuevas instancias desde la AMI. En el caso de las flotas configuradas para mantener la capacidad de destino, esta capacidad no se mantendrá.

c. (Opcional) En Nombre del par de claves, seleccione un par de claves existente o cree uno nuevo.

   [Par de claves existente] Elija el par de claves.

   [Nuevo par de claves] Elija Crear un nuevo par de claves para ir a la consola de Pares de claves. Cuando haya terminado, regrese a la página Solicitudes de spot y actualice la lista.

d. (Opcional) Expanda Entradas de inicialización adicionales y haga lo siguiente.

   i. (Opcional) Para habilitar la optimización de Amazon EBS, elija Iniciar instancias optimizadas para EBS en Optimizada para EBS.

   ii. (Opcional) Para añadir almacenamiento por bloques temporal para las instancias, elija Asociar al iniciar para Almacén de instancias.

   iii. (Opcional) Para agregar almacenamiento, elija Agregar nuevo volumen y especifique volúmenes de almacenamiento de instancias o volúmenes de Amazon EBS adicionales según el tipo de instancia.

   iv. (Opcional) De forma predeterminada, se habilita la monitorización básica para sus instancias. Para habilitar el monitoreo detallado, en Supervisión, elija Habilitar monitoreo detallado de CloudWatch.

   v. (Opcional) Para ejecutar una instancia de spot dedicada, elija Dedicada: ejecutar una instancia dedicada en Tenencia.

   vi. (Opcional) En Grupos de seguridad, elija uno o varios grupos de seguridad o cree uno nuevo.

[Grupo de seguridad existente] Elija uno o varios grupos de seguridad.

[Nuevo grupo de seguridad] Elija Crear nuevo grupo de seguridad para ir a la página Grupos de seguridad. Cuando haya terminado, vuelva a Solicitudes de spot y actualice la lista.

vii. (Opcional) Para poder acceder a las instancias desde Internet, elija Habilitar para Asignar IP pública IPv4 de forma automática.

viii. (Opcional) Para iniciar las instancias de spot con un rol de IAM, elija el rol para Perfil de instancia de IAM.

ix. (Opcional) Para ejecutar un script de inicio, cópielo en Datos de usuario.

x. (Opcional) Para agregar una etiqueta, elija Crear etiqueta, ingrese la clave y el valor de la etiqueta y elija Crear. Repita este proceso para cada etiqueta.

Para cada etiqueta, y a fin de etiquetar las instancias y la solicitud de flota de spot con la misma etiqueta, asegúrese de que tanto Instancias como Flota estén seleccionadas. Para solo etiquetar las instancias que inicia la flota, desmarque Flota. Para etiquetar solo la solicitud de flota de spot, desmarque Instancias.

5. Para Detalles adicionales de la solicitud, haga lo siguiente:

a. Revise los detalles adicionales de la solicitud. Para realizar cambios, borre Aplicar valores predeterminados.

b. (Opcional) Para Rol de flota de IAM, puede usar el rol predeterminado o elegir un rol distinto. Elija Usar rol predeterminado para utilizar el rol predeterminado tras modificar el rol.

c. (Opcional) En Precio máximo, puede usar el precio máximo predeterminado (el precio bajo demanda) o especificar el precio máximo que está dispuesto a pagar. Las instancias de spot no se iniciarán si el precio máximo es inferior al precio de spot de los tipos de instancias seleccionados.

d. (Opcional) Para crear una solicitud que solo sea válida durante un periodo específico, edite Solicitud válida desde y Solicitud válida hasta.

e. (Opcional) De forma predeterminada, terminamos las instancias de spot cuando caduca la solicitud de flota de spot. Para que sigan ejecutándose después de que caduque la solicitud, desactive Terminar las instancias cuando caduque la solicitud.

f. (Opcional) Para registrar las instancias de spot con un equilibrador de carga, elija Recibir tráfico de uno o varios balanceadores de carga y, a continuación, seleccione uno o varios Classic Load Balancers o grupos de destino.

6. En Unidad de computación mínima, elija las especificaciones de hardware mínimas (CPU virtuales, memoria y almacenamiento) que necesita para su aplicación o tarea, ya sea como especificaciones o como tipo de instancia.

   - Para como especificaciones, especifique el número de CPU virtuales requerido y la cantidad de memoria.
   - Para como tipo de instancia, acepte el tipo de instancia predeterminado o seleccione Cambiar tipo de instancia para elegir un tipo de instancia distinto.

7. En Capacidad de destino, haga lo siguiente:

   a. En Capacidad de destino total, especifique el número de unidades que desea solicitar. Para el tipo de unidad, puede elegir Instances (Instancias), vCPU o Memory (MiB) (Memoria [MiB]). Para especificar una capacidad de destino de 0 y añadir capacidad más tarde, elija Mantener capacidad de destino.

   b. (Opcional) En Incluir la capacidad base bajo demanda, especifique el número de unidades bajo demanda que desea solicitar. El número debe ser menor que la capacidad total de destino. Amazon EC2 calcula la diferencia y la asigna a unidades de spot para la solicitud.

      > **Important**
      >
      > Para especificar la capacidad bajo demanda opcional, primero debe elegir una plantilla de inicialización.

   c. (Opcional) De forma predeterminada, Amazon EC2 termina las instancias de spot cuando se interrumpen. Para mantener la capacidad de destino, seleccione Mantener la capacidad de destino. A continuación podrá especificar que Amazon EC2 finalice, detenga o hiberne las instancias de spot cuando se interrumpan. Para hacerlo, elija la opción correspondiente en Comportamiento de interrupción.

      > **Note**
      >
      > Si se anula o inhabilita una AMI especificada en los parámetros de inicialización, no se podrán iniciar nuevas instancias desde la AMI. En el caso de las flotas configuradas para mantener la capacidad de destino, esta capacidad no se mantendrá.

d. (Opcional) Para permitir que la flota de spot lance una instancia de spot de reemplazo cuando se emite una notificación de reequilibrio de instancia para una instancia de spot existente en la flota, seleccione Reequilibrio de capacidad y luego elija una estrategia de reemplazo de instancia. Si elige Iniciar antes de terminar, especifique el retraso (en segundos) antes de que la flota de spot termine las instancias anteriores. Para obtener más información, consulte Reequilibrio de la capacidad.

e. (Opcional) A fin de controlar la cantidad que paga por hora por todas las instancias de spot de su flota, seleccione Establecer el costo máximo para las instancias de spot y luego, ingrese la cantidad total máxima que está dispuesto a pagar por hora. Cuando se alcanza la cantidad total máxima, la flota de spot detiene la inicialización de instancias de spot, incluso si no se ha alcanzado la capacidad de destino. Para obtener más información, consulte Control de gastos.

8. En Red, haga lo siguiente:

   a. En Red, seleccione una VPC existente o cree una nueva.

      [VPC existente] Elija el VPC.

      [Nueva VPC] Elija Crear nueva VPC para ir a la consola de Amazon VPC. Cuando haya terminado, vuelva al asistente y actualice la lista.

   b. (Opcional) En Zona de disponibilidad, deje que AWS elija las zonas de disponibilidad para las instancias de spot. Si lo prefiere, puede especificar una o más zonas de disponibilidad.

      Si tiene más de una subred en una zona de disponibilidad, elija la subred adecuada en Subred. Para añadir subredes, elija Crear subred nueva para ir a la consola de Amazon VPC. Cuando haya terminado, vuelva al asistente y actualice la lista.

9. En Requisitos de tipo de instancia, puede especificar atributos de instancia y permitir que Amazon EC2 identifique los tipos de instancias óptimos con estos atributos, o puede especificar una lista de instancias. Para obtener más información, consulte Selección de tipo de instancia basada en atributos para la flota de spot.

   a. Si elige Especificar los atributos de instancia que coinciden con los requisitos de computación, especifique los atributos de instancia de la siguiente manera:

      i. En vCPU, ingrese el número mínimo y máximo deseado de vCPU. Para no especificar ningún límite, seleccione No minimum (Sin mínimo), No maximum (Sin máximo) o ambos.

ii. En Memory (GiB) (Memoria [GiB]), ingrese la cantidad mínima y máxima de memoria deseada. Para no especificar ningún límite, seleccione No minimum (Sin mínimo), No maximum (Sin máximo) o ambos.

iii. (Opcional) En Additional instance attributes (Atributos de instancia adicionales), puede especificar opcionalmente uno o varios atributos para expresar sus requisitos de computación con más detalle. Cada atributo adicional agrega una restricción más a su solicitud. Puede omitir los atributos adicionales; si se omiten, se utilizan los valores predeterminados. Para obtener una descripción de cada atributo y de sus valores predeterminados, consulte get-spot-placement-scores en la Referencia de la línea de comandos de Amazon EC2.

iv. (Opcional) Para ver los tipos de instancia con los atributos especificados, expanda Vista previa de los tipos de instancia que coinciden. Para excluir que los tipos de instancias se utilicen en la solicitud, seleccione las instancias y, a continuación, elija Excluir los tipos de instancias seleccionados.

b. Si elige Seleccionar los tipos de instancias de forma manual, la flota de spot proporciona una lista predeterminada de tipos de instancias. Para seleccionar más tipos de instancia, elija Agregar tipos de instancia, seleccione los tipos de instancias que desea utilizar en la solicitud y elija Seleccionar. Para eliminar tipos de instancias, seleccione los tipos de instancias y elija Eliminar.

10. En Estrategia de asignación, elija la estrategia que se ajuste a sus necesidades. Para obtener más información, consulte Estrategias de asignación de instancias de spot.
11. En Resumen de su solicitud de flota, revise la configuración de la flota y realice los ajustes si es necesario.
12. (Opcional) Para descargar una copia de la configuración de inicialización para utilizarla con la AWS CLI, elija Configuración de JSON.
13. Elija Iniciar.

    El tipo de solicitud de flota de spot es `fleet`. Cuando se atiende la solicitud, se añaden solicitudes de tipo `instance`, donde el estado es `active` y `fulfilled`.

Creación de una flota de spot mediante la AWS CLI

Para crear una solicitud de flota de spot mediante la AWS CLI

- Utilice el comando request-spot-fleet para crear una solicitud de flota de spot.

```
aws ec2 request-spot-fleet --spot-fleet-request-config file://config.json
```

Para ver archivos de configuración de ejemplo, consulte Configuraciones de ejemplo de flota de spot.

A continuación, se muestra un ejemplo del resultado:

```
{
    "SpotFleetRequestId": "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE"
}
```

Etiquetado de una flota de spot

Para ayudarlo a categorizar y administrar las solicitudes de flota de spot, puede etiquetarlas con metadatos personalizados. Puede asignar una etiqueta a una solicitud de flota de spot cuando la cree o posteriormente. Puede asignar etiquetas mediante la consola de Amazon EC2 o una herramienta de línea de comandos.

Cuando etiquete una solicitud de flota de spot, las instancias y los volúmenes iniciados por la flota de spot no se etiquetan automáticamente. Tiene que etiquetar explícitamente las instancias y los volúmenes que inicia la flota de spot. Puede elegir asignar etiquetas solo a la solicitud de flota de spot, solo a las instancias iniciadas por la flota, solo a los volúmenes adjuntados a las instancias iniciadas por la flota o a las tres.

> **Note**
>
> Las etiquetas de volumen solo se admiten para los volúmenes a los que se asocian Instancias bajo demanda. No se pueden etiquetar los volúmenes que están asociados a instancias de spot.

Para obtener más información sobre cómo funcionan las etiquetas, consulte Etiquetar los recursos de Amazon EC2.

Contenido

- Visualización de etiquetas de solicitud de flota de spot

Requisito previo

Otorgue al usuario el permiso para etiquetar recursos. Para obtener más información, consulte Ejemplo: Etiquetar recursos.

Para conceder a un usuario el permiso para etiquetar recursos

Cree una política de IAM que incluya lo siguiente:

- La acción `ec2:CreateTags`. Esto concede al usuario permiso para crear etiquetas.
- La acción `ec2:RequestSpotFleet`. Esto concede al usuario de IAM permiso para crear una solicitud de flota de spot.
- Para `Resource`, debe especificar `"*"`. Esto permite a los usuarios etiquetar todos los tipos de recursos.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "TagSpotFleetRequest",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags",
                "ec2:RequestSpotFleet"
            ],
            "Resource": "*"
        }
    ]
}
```

Important

Actualmente, no admitimos permisos de nivel de recursos para el recurso `spot-fleet-request`. Si especifica `spot-fleet-request` como recurso, obtendrá una excepción no autorizada cuando intente etiquetar la flota. En el ejemplo siguiente se muestra cómo no establecer la política.

```
{
    "Effect": "Allow",
    "Action": [
        "ec2:CreateTags",
        "ec2:RequestSpotFleet"
    ],
    "Resource": "arn:aws:ec2:us-east-1:111122223333:spot-fleet-request/*"
}
```

Para dar acceso, agregue permisos a los usuarios, grupos o roles:

- Usuarios y grupos en AWS IAM Identity Center:

  Cree un conjunto de permisos. Siga las instrucciones de Creación de un conjunto de permisos en la Guía del usuario de AWS IAM Identity Center.

- Usuarios administrados en IAM a través de un proveedor de identidades:

  Cree un rol para la federación de identidades. Siga las instrucciones descritas en Creación de un rol para un proveedor de identidad de terceros (federación) en la Guía del usuario de IAM.

- Usuarios de IAM:
  - Cree un rol que el usuario pueda aceptar. Siga las instrucciones descritas en Creación de un rol para un usuario de IAM en la Guía del usuario de IAM.
  - (No recomendado) Adjunte una política directamente a un usuario o añada un usuario a un grupo de usuarios. Siga las instrucciones descritas en Adición de permisos a un usuario (consola) de la Guía del usuario de IAM.

Etiquetado de una nueva flota de spot

Para etiquetar una nueva solicitud de flota de spot mediante la consola

1. Siga el procedimiento indicado en Creación de una solicitud de flota de spot con los parámetros definidos (consola).
2. Para agregar una etiqueta, expanda Configuraciones adicionales, elija Agregar nueva etiqueta y escriba la clave y el valor de la etiqueta. Repita este proceso para cada etiqueta.

Para cada etiqueta, puede etiquetar la solicitud de flota de spot y las instancias con la misma etiqueta. Para etiquetar ambas, asegúrese de que Etiquetas de instancia y Etiquetas de flota estén seleccionadas. Para etiquetar solo la solicitud de flota de spot, desactive Etiquetas de instancia. Para etiquetar solo las instancias iniciadas por la flota, desactive Etiquetas de flota.

3. Rellene los campos necesarios para crear una solicitud de flota de spot y, a continuación, elija Iniciar. Para obtener más información, consulte Creación de una solicitud de flota de spot con los parámetros definidos (consola).

Para etiquetar una solicitud nueva de flota de spot mediante la AWS CLI

Para etiquetar una solicitud de flota de spot al momento de crearla, configure la solicitud de flota de spot de la siguiente manera:

- Especifique las etiquetas para la solicitud de flota de spot en `SpotFleetRequestConfig`.
- En `ResourceType`, especifique `spot-fleet-request`. Si especifica otro valor, la solicitud de flota devolverá un error.
- Para `Tags`, especifique el par clave-valor. Puede especificar más de un par clave-valor.

En el ejemplo siguiente, la solicitud de flota de spot se etiqueta con dos etiquetas: Key=Environment y Value=Production, y Key=Cost-Center y Value=123.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchSpecifications": [
            {
                "ImageId": "ami-0123456789EXAMPLE",
                "InstanceType": "c4.large"
            }
        ],
        "SpotPrice": "5",
        "TargetCapacity": 2,
        "TerminateInstancesWithExpiration": true,
        "Type": "maintain",
        "ReplaceUnhealthyInstances": true,
```

```
        "InstanceInterruptionBehavior": "terminate",
        "InstancePoolsToUseCount": 1,
        "TagSpecifications": [
            {
                "ResourceType": "spot-fleet-request",
                "Tags": [
                    {
                        "Key": "Environment",
                        "Value":"Production"
                    },
                    {
                        "Key": "Cost-Center",
                        "Value":"123"
                    }
                ]
            }
        ]
    }
}
```

Etiquetado de una flota de spot nueva y las instancias y los volúmenes que inicia

Para etiquetar una solicitud nueva de flota de spot y las instancias y los volúmenes que inicia mediante la AWS CLI

Para etiquetar una solicitud de flota de spot al momento de crearla y para etiquetar las instancias y los volúmenes cuando la flota los inicia, ajuste la configuración de la solicitud de flota de spot de la siguiente manera:

Etiquetas de solicitud de flota de spot:

- Especifique las etiquetas para la solicitud de flota de spot en `SpotFleetRequestConfig`.
- En `ResourceType`, especifique `spot-fleet-request`. Si especifica otro valor, la solicitud de flota devolverá un error.
- Para `Tags`, especifique el par clave-valor. Puede especificar más de un par clave-valor.

Etiquetas de instancia:

- Especifique las etiquetas para las instancias en `LaunchSpecifications`.
- En `ResourceType`, especifique `instance`. Si especifica otro valor, la solicitud de flota devolverá un error.

- Para `Tags`, especifique el par clave-valor. Puede especificar más de un par clave-valor.

  También puede especificar las etiquetas de la instancia en la plantilla de inicialización a la que se hace referencia en la solicitud de flota de spot.

Etiquetas de volumen:

- Especifique las etiquetas para los volúmenes de la plantilla de inicialización a la que se hace referencia en la solicitud de flota de spot. No se admite el etiquetado de volumen en `LaunchSpecifications`.

En el ejemplo siguiente, la solicitud de flota de spot se etiqueta con dos etiquetas: Key=Environment y Value=Production, y Key=Cost-Center y Value=123. Las instancias iniciadas por la flota están etiquetadas con una etiqueta (que es la misma que una de las etiquetas para la solicitud de flota de spot): Key=Cost-Center y Value=123.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchSpecifications": [
            {
                "ImageId": "ami-0123456789EXAMPLE",
                "InstanceType": "c4.large",
                "TagSpecifications": [
                    {
                        "ResourceType": "instance",
                        "Tags": [
                            {
                                "Key": "Cost-Center",
                                "Value": "123"
                            }
                        ]
                    }
                ]
            }
        ],
        "SpotPrice": "5",
        "TargetCapacity": 2,
```

```
        "TerminateInstancesWithExpiration": true,
        "Type": "maintain",
        "ReplaceUnhealthyInstances": true,
        "InstanceInterruptionBehavior": "terminate",
        "InstancePoolsToUseCount": 1,
        "TagSpecifications": [
            {
                "ResourceType": "spot-fleet-request",
                "Tags": [
                    {
                        "Key": "Environment",
                        "Value":"Production"
                    },
                    {
                        "Key": "Cost-Center",
                        "Value":"123"
                    }
                ]
            }
        ]
    }
}
```

Para etiquetar instancias iniciadas por una flota de spot mediante la AWS CLI

Para etiquetar instancias cuando la flota las inicia, puede especificar las etiquetas en la plantilla de inicialización a la que se hace referencia en la solicitud de flota de spot, o bien especificar las etiquetas en la configuración de la solicitud de flota de spot de la siguiente manera:

- Especifique las etiquetas para las instancias en `LaunchSpecifications`.
- En `ResourceType`, especifique `instance`. Si especifica otro valor, la solicitud de flota devolverá un error.
- Para `Tags`, especifique el par clave-valor. Puede especificar más de un par clave-valor.

En el ejemplo siguiente, las instancias iniciadas por la flota se etiquetan con una etiqueta: Key=Cost-Center y Value=123.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
```

```
        "IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchSpecifications": [
            {
                "ImageId": "ami-0123456789EXAMPLE",
                "InstanceType": "c4.large",
                "TagSpecifications": [
                    {
                        "ResourceType": "instance",
                        "Tags": [
                            {
                                "Key": "Cost-Center",
                                "Value": "123"
                            }
                        ]
                    }
                ]
            }
        ],
        "SpotPrice": "5",
        "TargetCapacity": 2,
        "TerminateInstancesWithExpiration": true,
        "Type": "maintain",
        "ReplaceUnhealthyInstances": true,
        "InstanceInterruptionBehavior": "terminate",
        "InstancePoolsToUseCount": 1
    }
}
```

Para etiquetar volúmenes adjuntados a instancias bajo demanda iniciadas por una flota de spot mediante la AWS CLI

Para etiquetar volúmenes cuando los crea la flota, debe especificar las etiquetas en la plantilla de inicialización a la que se hace referencia en la solicitud de flota de spot.

> **Note**
>
> Las etiquetas de volumen solo se admiten para los volúmenes a los que se asocian Instancias bajo demanda. No se pueden etiquetar los volúmenes que están asociados a Instancias de spot.
> No se admite el etiquetado de volumen en `LaunchSpecifications`.

Etiquetado de una flota de spot existente

Para etiquetar una solicitud de flota de spot existente mediante la consola

Después de crear una solicitud de flota de spot, puede agregar etiquetas a la solicitud de flota mediante la consola.

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Spot Requests (Solicitudes de spot).
3. Seleccione la solicitud de flota de spot.
4. Elija la pestaña Tags (Etiquetas) y, a continuación, Create Tag (Crear etiqueta).

Para etiquetar una solicitud de flota de spot existente mediante la AWS CLI

Puede utilizar el comando create-tags para etiquetar recursos existentes. En el ejemplo siguiente, la solicitud de flota de spot existente se etiqueta con Key=purpose y Value=test.

```
aws ec2 create-tags \
    --resources sfr-11112222-3333-4444-5555-66666EXAMPLE \
    --tags Key=purpose,Value=test
```

Visualización de etiquetas de solicitud de flota de spot

Para ver las etiquetas de solicitud de flota de spot mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Solicitudes de spot.
3. Seleccione su solicitud de flota de spot y elija la pestaña Etiquetas.

Para describir las etiquetas de solicitud de flota de spot

Utilice el comando describe-tags para ver las etiquetas del recurso especificado. En el siguiente ejemplo, describe las etiquetas para la solicitud de flota de spot especificada.

```
aws ec2 describe-tags \
    --filters "Name=resource-id,Values=sfr-11112222-3333-4444-5555-66666EXAMPLE"
```

```
{
```

```
    "Tags": [
        {
            "Key": "Environment",
            "ResourceId": "sfr-11112222-3333-4444-5555-66666EXAMPLE",
            "ResourceType": "spot-fleet-request",
            "Value": "Production"
        },
        {
            "Key": "Another key",
            "ResourceId": "sfr-11112222-3333-4444-5555-66666EXAMPLE",
            "ResourceType": "spot-fleet-request",
            "Value": "Another value"
        }
    ]
}
```

También puede ver las etiquetas de una solicitud de flota de spot mediante la descripción de la solicitud de flota de spot.

Utilice el comando describe-spot-fleet-requests para ver la configuración de la solicitud de flota de spot especificada, que incluye las etiquetas especificadas para la solicitud de la flota.

```
aws ec2 describe-spot-fleet-requests \
    --spot-fleet-request-ids sfr-11112222-3333-4444-5555-66666EXAMPLE
```

```
{
    "SpotFleetRequestConfigs": [
        {
            "ActivityStatus": "fulfilled",
            "CreateTime": "2020-02-13T02:49:19.709Z",
            "SpotFleetRequestConfig": {
                "AllocationStrategy": "capacityOptimized",
                "OnDemandAllocationStrategy": "lowestPrice",
                "ExcessCapacityTerminationPolicy": "Default",
                "FulfilledCapacity": 2.0,
                "OnDemandFulfilledCapacity": 0.0,
                "IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-
tagging-role",
                "LaunchSpecifications": [
                    {
                        "ImageId": "ami-0123456789EXAMPLE",
                        "InstanceType": "c4.large"
```

```
                    }
                ],
                "TargetCapacity": 2,
                "OnDemandTargetCapacity": 0,
                "Type": "maintain",
                "ReplaceUnhealthyInstances": false,
                "InstanceInterruptionBehavior": "terminate"
            },
            "SpotFleetRequestId": "sfr-11112222-3333-4444-5555-66666EXAMPLE",
            "SpotFleetRequestState": "active",
            "Tags": [
                {
                    "Key": "Environment",
                    "Value": "Production"
                },
                {
                    "Key": "Another key",
                    "Value": "Another value"
                }
            ]
        }
    ]
}
```

Descripción de la flota de spot

La flota de spot inicia instancias de spot siempre que su precio máximo sea superior al precio de spot y haya capacidad disponible. Las instancias de spot se ejecutan hasta que se interrumpen o las termina el usuario.

Para describir la flota de spot (consola)

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Spot Requests (Solicitudes de spot).
3. Seleccione la solicitud de flota de spot. Para ver los detalles de configuración, elija Descripción.
4. Para enumerar las instancias de spot de la flota de spot, elija Instancias.
5. Para ver el historial de la flota de spot, elija Historial.

Para describir la flota de spot (AWS CLI)

Utilice el comando describe-spot-fleet-requests para describir las solicitudes de flota de spot.

```
aws ec2 describe-spot-fleet-requests
```

Utilice el comando describe-spot-fleet-instances para describir las instancias de spot de la flota de spot especificada.

```
aws ec2 describe-spot-fleet-instances \
    --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE
```

Utilice el comando describe-spot-fleet-request-history para describir el historial de la solicitud de flota de spot especificada.

```
aws ec2 describe-spot-fleet-request-history \
    --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --start-time 2015-05-18T00:00:00Z
```

Modificación de una solicitud de flota de spot

Puede modificar una solicitud de flota de spot activa para completar las siguientes tareas:

- Aumentar la capacidad de destino y la parte bajo demanda
- Disminuir la capacidad de destino y la parte bajo demanda

> **Note**
>
> No se puede modificar una solicitud de flota de spot puntual. Solo puede modificar una solicitud de flota de spot si seleccionó Mantener la capacidad de destino cuando creó la solicitud de flota de spot.

Cuando se aumenta la capacidad de destino, la flota de spot inicia instancias de spot adicionales. Cuando se aumenta la parte bajo demanda, la flota de spot inicia instancias bajo demanda adicionales.

Cuando se aumenta la capacidad de destino, la flota de spot inicia las instancias de spot adicionales de acuerdo con la estrategia de asignación de la solicitud de la flota de spot.

Cuando se reduce la capacidad de destino, la flota de spot cancela cualquier solicitud abierta que supere la nueva capacidad de destino. Puede solicitar que la flota de spot termine las instancias

de spot hasta que el tamaño de la flota alcance la nueva capacidad de destino. Si la estrategia de asignación es `diversified`, la flota de spot termina instancias de los distintos grupos. También puede solicitar que la flota de spot mantenga la flota con su tamaño actual, pero que no reemplace ninguna de las instancias de spot que se hayan interrumpido ni que el usuario haya terminado manualmente.

Cuando una flota de spot termina una instancia porque se ha reducido la capacidad de destino, la instancia recibe un aviso de interrupción de instancia de spot.

Para modificar una solicitud de flota de spot (consola)

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Spot Requests (Solicitudes de spot).
3. Seleccione la solicitud de flota de spot.
4. Elija Acciones y, a continuación, Modificar capacidad de destino.
5. En Modificar capacidad de destino, haga lo siguiente:
    a. Introduzca la nueva capacidad de destino y la parte bajo demanda
    b. (Opcional) Si está disminuyendo la capacidad de destino, pero quiere conservar el tamaño actual de la flota, borre Terminar instancias.
    c. Elija Submit.

Para modificar una solicitud de flota de spot mediante la AWS CLI

Utilice el comando modify-spot-fleet-request para actualizar la capacidad de destino de la solicitud de flota de spot especificada.

```
aws ec2 modify-spot-fleet-request \
    --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --target-capacity 20
```

Puede modificar el comando anterior de la siguiente manera para disminuir la capacidad de destino de la flota de spot especificada sin que ello suponga terminar ninguna de las instancias de spot.

```
aws ec2 modify-spot-fleet-request \
    --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --target-capacity 10 \
    --excess-capacity-termination-policy NoTermination
```

Cancelación de una solicitud de flota de spot

Si ya no necesita una flota de spot, puede cancelar la solicitud de la flota de spot. Tras cancelar una solicitud de flota, todas las solicitudes de spot asociadas con la flota también se cancelan, de forma que no se iniciará ninguna instancia de spot nueva.

Al cancelar una solicitud de flota de spot, debe especificar si desea terminar también todas sus instancias. Esto incluye tanto las instancias bajo demanda como las instancias de spot.

Si especifica que se terminen las instancias cuando se cancele la solicitud de flota, esta pasará al estado `cancelled_terminating`. En caso contrario, la solicitud de flota pasa al estado `cancelled_running` y las instancias seguirán ejecutándose hasta que se interrumpan o las termine manualmente.

Restricciones

- Puede eliminar hasta 100 flotas en una sola solicitud. Si supera la cantidad especificada, no se eliminan las flotas.

Para cancelar una solicitud de flota de spot (consola)

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Spot Requests (Solicitudes de spot).
3. Seleccione la solicitud de flota de spot.
4. Elija Acciones, Cancelar comando.
5. En el cuadro de diálogo Cancelar solicitudes de spot, haga lo siguiente:
    a. Para terminar las instancias asociadas al mismo tiempo que se cancela la solicitud de flota de spot, deje seleccionada la casilla Terminar instancias. Para cancelar la solicitud de flota de spot sin terminar las instancias asociadas, desmarque la casilla Terminar instancias.
    b. Elija Confirmar.

Para cancelar una solicitud de flota de spot y terminar sus instancias mediante la AWS CLI

Utilice el comando cancel-spot-fleet-requests (cancelar las solicitudes de la flota de spot) para cancelar la solicitud de flota de spot especificada y terminar las instancias.

```
aws ec2 cancel-spot-fleet-requests \
```

```
    --spot-fleet-request-ids sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --terminate-instances
```

Ejemplo de resultado

```
{
    "SuccessfulFleetRequests": [
        {
            "SpotFleetRequestId": "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE",
            "CurrentSpotFleetRequestState": "cancelled_terminating",
            "PreviousSpotFleetRequestState": "active"
        }
    ],
    "UnsuccessfulFleetRequests": []
}
```

Para cancelar una solicitud de flota de spot sin terminar sus instancias mediante la AWS CLI

Puede modificar el comando anterior con el parámetro `--no-terminate-instances` para cancelar la solicitud de flota de spot especificada sin terminar sus instancias de spot y bajo demanda.

```
aws ec2 cancel-spot-fleet-requests \
    --spot-fleet-request-ids sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --no-terminate-instances
```

Ejemplo de resultado

```
{
    "SuccessfulFleetRequests": [
        {
            "SpotFleetRequestId": "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE",
            "CurrentSpotFleetRequestState": "cancelled_running",
            "PreviousSpotFleetRequestState": "active"
        }
    ],
    "UnsuccessfulFleetRequests": []
}
```

Métricas de CloudWatch para las flotas de spot

Amazon EC2 proporciona métricas de Amazon CloudWatch que puede utilizar para monitorear su flota de spot.

> **Important**
>
> Para asegurar la precisión, le recomendamos que habilite la monitorización detallada al usar estas métricas. Para obtener más información, consulte Activar o desactivar el monitoreo detallado para las instancias.

Para obtener más información sobre las métricas de CloudWatch que proporciona Amazon EC2, consulte Monitorear las instancias con CloudWatch.

Métricas de flota de spot

El espacio de nombres `AWS/EC2Spot` incluye las siguientes métricas, además de las métricas de CloudWatch para las instancias de spot de la flota. Para obtener más información, consulte Métricas de la instancia.

Métrica	Descripción
`AvailableInstancePoolsCount`	Grupos de capacidad de spot especificados en la solicitud de flota de spot. Unidades: recuento
`BidsSubmittedForCapacity`	La capacidad por la que Amazon EC2 ha enviado solicitudes de flota de spot. Unidades: recuento
`EligibleInstancePoolCount`	Los grupos de capacidad de spot especificados en la solicitud de flota de spot en los que Amazon EC2 pueda gestionar solicitudes. Amazon EC2 no gestiona las solicitud es de grupos en los que el precio máximo que esté dispuesto a pagar por instancias de spot sea menor que el precio de spot o en los que el precio de spot sea mayor que el precio de las instancias bajo demanda. Unidades: recuento

Métrica	Descripción
FulfilledCapacity	La capacidad satisfecha por Amazon EC2. Unidades: recuento
MaxPercentCapacityAllocation	El valor máximo de PercentCapacityAllocation en todos los grupos de flota de spot especificados en la solicitud de flota de spot. Unidades: porcentaje
PendingCapacity	La diferencia entre TargetCapacity y FulfilledCapacity . Unidades: recuento
PercentCapacityAllocation	La capacidad asignada al grupo para las dimensiones especificadas. Para obtener el valor máximo registrado en todos los grupos de capacidad de spot, use MaxPercentCapacityAllocation . Unidades: porcentaje
TargetCapacity	La capacidad de destino de la solicitud de flota de spot. Unidades: recuento
TerminatingCapacity	Capacidad que se va a terminar debido a que la capacidad aprovisionada es superior a la capacidad de destino. Unidades: recuento

Si la unidad de medida de una métrica es Count, la estadística más útil es Average.

Dimensiones de la flota de spot

Para filtrar los datos para una flota de spot, use las siguientes dimensiones.

Dimensiones	Descripción
`AvailabilityZone`	Filtra los datos por zona de disponibilidad.
`FleetRequestId`	Filtra los datos por solicitud de flota de instancias spot.
`InstanceType`	Filtra los datos por tipo de instancia.

Vea las métricas de CloudWatch para su flota de spot

Puede ver las métricas de CloudWatch para su flota de spot en la consola de Amazon CloudWatch. Estas métricas se muestran en gráficos de monitorización. Estos gráficos muestran puntos de datos si la flota de spot está activa.

Las métricas se agrupan en primer lugar por el espacio de nombres y, a continuación, por las diversas combinaciones de dimensiones dentro de cada espacio de nombres. Por ejemplo, puede ver todas las métricas de flota de spot o de los grupos de métricas de la flota de spot por ID de solicitud de flota de spot, tipo de instancia o zona de disponibilidad.

Para ver las métricas de la flota de spot

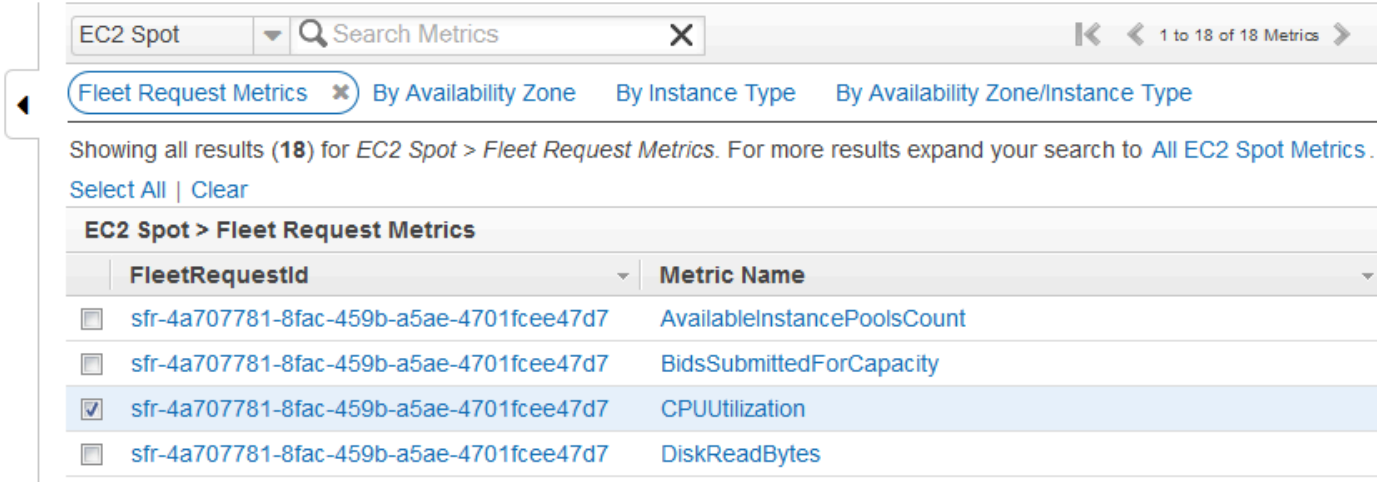
1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, seleccione Métricas.
3. Elija el espacio de nombres de métrica de EC2 Spot.

> **Note**
>
> Si no se muestra el espacio de nombres de EC2 Spot, puede haber dos motivos. Aún no utiliza la flota de spot: solo los servicios de AWS que está utilizando envían métricas a Amazon CloudWatch. O bien, si no ha utilizado la flota de spot durante las últimas dos semanas, el espacio de nombres no aparecerá.

4. (Opcional) Para filtrar las métricas por dimensión, seleccione una de las siguientes opciones:

   - Métricas de solicitud de flota: agrupar por solicitud de flota de spot
   - Por zona de disponibilidad: agrupar por solicitud de flota de spot y zona de disponibilidad
   - Por tipo de instancia: agrupar por solicitud de flota de spot y tipo de instancia
   - Por zona de disponibilidad/tipo de instancia: agrupar por solicitud de flota de spot, zona de disponibilidad y tipo de instancia

5. Para ver los datos para una métrica, active la casilla de verificación situada junto a ella.



Escalado automático para la flota de spot

El escalado automático es la posibilidad de aumentar o disminuir la capacidad de destino de una flota de spot de forma automática en función de la demanda. Una flota de spot puede iniciar instancias (escalado ascendente) o terminar instancias (escalado horizontal), dentro del rango que elija, en respuesta a una o varias políticas de escalado.

La flota de spot admite los siguientes tipos de escalado automático:

- Escalado de seguimiento de destino: permite aumentar o reducir la capacidad actual de la flota en función de un valor de destino especificado en una métrica determinada. Funciona de forma similar a los termostatos, que mantienen la temperatura del hogar — el usuario selecciona una temperatura y el termostato hace el resto.
- Escalado por pasos: permite aumentar o reducir la capacidad actual de la flota en función de una serie de ajustes de escalado, denominados ajustes por pasos, que varían en función del tamaño de la interrupción de alarma.

- Escalado programado: permite aumentar o reducir la capacidad actual de la flota en función de la fecha y la hora.

Si utiliza la ponderación de instancias, recuerde que la flota de spot puede superar la capacidad de destino según sea necesario. La capacidad utilizada puede ser un número de coma flotante, pero la capacidad de destino debe ser un número entero, por lo que la flota de spot redondea hacia arriba al siguiente entero. Debe tener en cuenta estos comportamientos cuando observe los resultados de una política de escalado después de dispararse una alarma. Por ejemplo, suponga que la capacidad de destino es de 30, la capacidad atendida es de 30,1 y la política de escalado resta 1. Cuando se dispara la alarma, el proceso de escalado automático resta 1 a 30,1, que da 29,1; así que al redondear hacia arriba, el resultado es 30, por lo que no se realiza ninguna acción de escalado. Veamos otro ejemplo: supongamos que seleccionó ponderaciones de instancias de 2, 4 y 8, y una capacidad de destino de 10, pero no había disponible ninguna instancia con ponderación 2, por lo que la flota de spot aprovisionó instancias de ponderaciones 4 y 8, que producen una capacidad utilizada de 12. Si la política de escalado disminuye la capacidad de destino en un 20 % y se dispara una alarma, el proceso de escalado automático resta 12*0,2 de 12, que es igual a 9,6 y, al redondear hacia arriba, da 10, por lo que no se realiza ninguna acción de escalado.

Las políticas de escalado que crea para la flota de spot admiten un periodo de recuperación. Es el número de segundos después de completarse una actividad de escalado en que las actividades del escalado anterior relacionadas con un disparador pueden influir en los futuros eventos de escalado. Para políticas de escalado ascendente, mientras el periodo de recuperación está en vigor, la capacidad que se agregó en el anterior evento de escalado ascendente que inició la recuperación se calcula como parte de la capacidad deseada para el siguiente escalado ascendente. La intención es realizar continuamente (pero no excesivamente) un escalado ascendente. Para políticas de escalado descendente, el periodo de recuperación se usa para bloquear subsiguientes solicitudes de escalado descendente hasta que haya caducado. La intención es realizar un escalado descendente de manera conservadora para proteger la disponibilidad de la aplicación. No obstante, si otra alarma dispara una política de escalado ascendente durante el periodo de recuperación después de un escalado descendente, el escalado automático realiza inmediatamente un escalado ascendente del destino escalable.

Le recomendamos realizar el escalado según métricas de instancia cuya frecuencia sea de un minuto, ya que esto garantiza una respuesta más rápida a los cambios de utilización. Realizar el escalado utilizando métricas con una frecuencia de 5 minutos puede generar un tiempo de respuesta más lento y hacer que el escalado se realice con datos de métricas que están obsoletos. Para enviar los datos de las métricas de la instancia a CloudWatch en periodos de 1 minuto, puede habilitar una

monitorización detallada específicamente para la instancia. Para obtener más información, consulte Activar o desactivar el monitoreo detallado para las instancias y Creación de una solicitud de flota de spot con los parámetros definidos (consola).

Para obtener más información acerca de la configuración de escalado de la flota de spot, consulte los siguientes recursos:

- Sección application-autoscaling de la Referencia de comandos de la AWS CLI
- Referencia de la API de Application Auto Scaling
- Guía del usuario de la aplicación Auto Scaling

Permisos de IAM necesarios para el escalado automático de la flota de spot

El escalado automático para la flota de spot es posible gracias a una combinación de las API de Amazon EC2, Amazon CloudWatch y Application Auto Scaling. Las solicitudes de flota de spot se crean con Amazon EC2, las alarmas se crean con CloudWatch y las políticas de escalado se crean con Application Auto Scaling.

Además de los permisos de IAM para la flota de spot y Amazon EC2, el usuario que accede a la configuración de escalado de la flota debe tener los permisos adecuados para los servicios que admiten el escalado dinámico. Los usuarios deben contar con los permisos necesarios para utilizar las acciones que se muestran en la siguiente política de ejemplo.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "application-autoscaling:*",
                "ec2:DescribeSpotFleetRequests",
                "ec2:ModifySpotFleetRequest",
                "cloudwatch:DeleteAlarms",
                "cloudwatch:DescribeAlarmHistory",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:DescribeAlarmsForMetric",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:ListMetrics",
                "cloudwatch:PutMetricAlarm",
                "cloudwatch:DisableAlarmActions",
```

```
                "cloudwatch:EnableAlarmActions",
                "iam:CreateServiceLinkedRole",
                "sns:CreateTopic",
                "sns:Subscribe",
                "sns:Get*",
                "sns:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

También puede crear sus propias políticas de IAM que permitan permisos más precisos para las llamadas a la API de Auto Scaling de aplicaciones. Para obtener más información, consulte Autenticación y control de acceso en la Guía del usuario de Auto Scaling de aplicaciones.

El servicio Application Auto Scaling también necesita permiso para describir sus flotas de spot y las alarmas de CloudWatch, así como permisos para modificar su capacidad de destino de la flota de spot en su nombre. Si habilita el escalado automático para su flota de spot, crea un rol vinculado a un servicio denominado `AWSServiceRoleForApplicationAutoScaling_EC2SpotFleetRequest`. Este rol vinculado a servicio concede a Auto Scaling de aplicaciones permiso para describir las alarmas de sus políticas, monitorizar la capacidad actual de la flota y modificar la capacidad de esta. El rol de flota de spot original administrado para Application Auto Scaling era `aws-ec2-spot-fleet-autoscale-role`, pero ya no es necesario. El rol vinculado al servicio es el rol predeterminado para Auto Scaling de aplicaciones. Para obtener más información, consulte Roles vinculados a servicios en la Guía del usuario de Auto Scaling de aplicaciones.

Escalado de una flota de spot con una política de seguimiento de destino

Las políticas de escalado de seguimiento de destino le permiten seleccionar una métrica y establecer un valor de destino. La flota de spot crea y administra las alarmas de CloudWatch que activan la política de escalado y calcula el ajuste de escalado en función de la métrica y el valor de objetivo. La política de escalado amplía o reduce la capacidad en función de las necesidades para mantener la métrica en el valor objetivo especificado o en un valor próximo. Además de mantener la métrica próxima al valor de destino, la política de escalado de seguimiento de destino también se ajusta a las fluctuaciones de la métrica producidas por patrones de carga fluctuante y minimiza las fluctuaciones rápidas de la capacidad de la flota.

Puede crear varias políticas de escalado de seguimiento de destino en una flota de spot, siempre que cada una de ellas utilice una métrica diferente. La flota se escala en función de la política que proporciona la mayor capacidad de flota. Esto le permite abordar diferentes situaciones y garantizar que siempre hay capacidad suficiente para procesar las cargas de trabajo de la aplicación.

Para garantizar la disponibilidad de la aplicación, la flota se escala en horizontal proporcionalmente a la métrica tan rápido como puede, pero se escala de forma descendente más gradualmente.

Cuando una flota de spot termina una instancia porque se ha reducido la capacidad de destino, la instancia recibe un aviso de interrupción de instancia de spot.

No modifique ni elimine las alarmas de CloudWatch que la flota de spot administra para las políticas de escalado de seguimiento de destino. La flota de spot elimina automáticamente las alarmas cuando se elimina la política de escalado de seguimiento de destino.

Limitación

La solicitud de flota de spot debe tener un tipo de solicitud de `maintain`. El escalado automático no se admite para solicitudes de tipo `request`.

Para configurar una política de seguimiento de destino (consola)

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Spot Requests (Solicitudes de spot).
3. Seleccione la solicitud de flota de spot y, a continuación, elija Auto Scaling.
4. Si el escalado automático no está configurado, elija Configurar.
5. Utilice Capacidad de escalado entre para establecer la capacidad mínima y máxima de la flota. El escalado automático no escalará la flota ni por debajo de la capacidad mínima ni por encima de la capacidad máxima.
6. En Nombre de política, escriba un nombre para la política.
7. Elija una métrica de destino en Métrica de destino.
8. Introduzca un Valor de destino para la métrica.
9. En Periodo de recuperación, especifique un nuevo valor (en segundos) o mantenga el valor predeterminado.
10. (Opcional) Seleccione Deshabilitar escalado descendente para omitir el paso de creación de una política de escalado descendente basada en la configuración actual. Puede crear una política de escalado descendente con una configuración diferente.

11. Seleccione Save.

Para configurar una política de escalado de seguimiento de destino mediante la AWS CLI

1. Registre la solicitud de flota de spot como un destino escalable mediante el comando register-scalable-target.
2. Cree una política de escalado mediante el comando put-scaling-policy.

Escalado de la flota de spot mediante políticas de escalado por pasos

Mediante políticas de escalado por pasos, puede especificar alarmas de CloudWatch para disparar el proceso de escalado. Por ejemplo, si desea realizar un escalado ascendente cuando el uso de la CPU alcance un determinado nivel, cree una alarma usando la métrica `CPUUtilization` que proporciona Amazon EC2.

Al crear una política de escalado por pasos, debe especificar uno de los siguientes tipos de ajuste de escalado:

- Agregar: permite aumentar la capacidad de destino de la flota en un número especificado de unidades de capacidad o un porcentaje especificado de la capacidad actual.
- Eliminar: permite disminuir la capacidad de destino de la flota en un número especificado de unidades de capacidad o un porcentaje especificado de la capacidad actual.
- Establecer en: permite establecer la capacidad de destino de la flota en el número especificado de unidades de capacidad.

Cuando se dispara una alarma, el proceso de escalado automático calcula la nueva capacidad de destino usando la capacidad atendida y la política de escalado y, a continuación, actualiza la capacidad de destino en consecuencia. Por ejemplo, suponga que la capacidad de destino y la capacidad atendida suman 10 y la política de escalado suma 1. Cuando se dispara la alarma, el proceso de escalado automático le agrega 1 a 10 para llegar a 11, de manera que la flota de spot inicia 1 instancia.

Cuando una flota de spot termina una instancia porque se ha reducido la capacidad de destino, la instancia recibe un aviso de interrupción de instancia de spot.

Limitación

La solicitud de flota de spot debe tener un tipo de solicitud de `maintain`. El escalado automático no se admite para solicitudes de tipo `request` o bloques de spot.

Requisitos previos

- Determine qué métricas CloudWatch son importantes para su aplicación. Puede crear alarmas de CloudWatch basadas en métricas proporcionadas por AWS o en sus propias métricas personalizadas.
- Para las métricas de AWS que utilizara en las políticas de escalado, habilite la recopilación de métricas de CloudWatch si el servicio que proporciona las métricas no la habilita de forma predeterminada.

Para crear una alarma de CloudWatch

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, elija Alarmas.
3. Elija Create alarm (Crear alarma).
4. En la página Especificar métricas y condiciones, elija Seleccionar métrica.
5. Elija Spot de EC2 y Métricas de solicitud de flota, seleccione una métrica (por ejemplo, TargetCapacity) y, a continuación, Seleccionar métrica.

   Aparece la página Especificar métrica y condiciones, que muestra un gráfico y otra información sobre la métrica que ha seleccionado.
6. En Periodo, elija el periodo de evaluación para la alarma, por ejemplo, 1 minuto. Al evaluar la alarma, cada periodo se agrega a un punto de datos.

   > **Note**
   >
   > Un periodo más corto crea una alarma con más sensibilidad.
7. En Condiciones, defina la alarma definiendo la condición del umbral. Por ejemplo, puede definir un umbral para activar la alarma cuando el valor de la métrica sea superior o igual al 80 %.
8. En Configuración adicional, para Puntos de datos para alarma, especifique el número de puntos de datos (periodos de evaluación) que debe haber en el estado ALARM para activar la alarma, por ejemplo, 1 período de evaluación o 2 de 3 períodos de evaluación. Esto crea una alarma que pasa al estado ALARM si se sobrepasan muchas periodos consecutivos. Para obtener más información, consulte Evaluación de una alarma en la Guía del usuario de Amazon CloudWatch.

9. Para Tratamiento de datos que faltan, elija una de las opciones (o deje el valor predeterminado de Tratar los datos que faltan como ausentes). Para obtener más información, consulte Configuración de cómo las alarmas de CloudWatch tratan los datos faltantes en la Guía del usuario de Amazon CloudWatch.
10. Seleccione Siguiente.
11. De forma opcional, para recibir una notificación de un evento de escalado, en Notificación, puede elegir o crear el tema de Amazon SNS que desea usar para recibir notificaciones. De lo contrario, puede eliminar la notificación ahora y añadir una más adelante si es necesario.
12. Seleccione Siguiente.
13. En Añadir una descripción, escriba el nombre y la descripción de la alarma y haga clic en Siguiente.
14. Elija Create alarm (Crear alarma).

Para configurar una política de escalado por pasos para su flota de spot (consola)

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Spot Requests (Solicitudes de spot).
3. Seleccione la solicitud de flota de spot y, a continuación, elija Auto Scaling.
4. Si el escalado automático no está configurado, elija Configurar.
5. Utilice Capacidad de escalado entre para establecer la capacidad mínima y máxima de la flota. Las políticas de escalado no reducirán la flota por debajo de la capacidad mínima ni la aumentarán por encima de la capacidad máxima.
6. En Políticas de escalado, Tipo de política, elija Política de escalado por pasos.
7. En un principio, Políticas de escalado contiene políticas de escalado por pasos denominadas ScaleUp y ScaleDown. Puede completar estas políticas o elegir Quitar política para eliminarlas. También puede elegir Añadir política.
8. Para definir una política, haga lo siguiente:

    a. En Policy name (Nombre de política), escriba un nombre para la política.
    b. En Disparador de política, seleccione una alarma ya establecida o elija Crear alarma para abrir la consola de Amazon CloudWatch y crear una alarma.
    c. En Modificar la capacidad, defina la cantidad que desea tener y los límites inferior y superior del ajuste por pasos. Puede agregar o eliminar un número específico de instancias o un porcentaje del tamaño de la flota existente, o establecer un tamaño exacto para la flota.

Por ejemplo, para crear una política de escalado por pasos que aumente la capacidad de la flota en un 30 por ciento, elija `Add`, escriba `30` en el siguiente campo y, a continuación, elija `percent`. De forma predeterminada, el límite inferior para Agregar política es el umbral de la alarma y el límite superior es infinito positivo (+). De forma predeterminada, el límite superior de Quitar política es el límite de la alarma y el límite inferior es infinito negativo (-).

d. (Opcional) Para agregar otro paso, elija Agregar paso.

e. En Periodo de recuperación, especifique un nuevo valor (en segundos) o mantenga el valor predeterminado.

9. Seleccione Guardar.

Para configurar políticas de escalado por pasos para la flota de spot mediante la AWS CLI

1. Registre la solicitud de flota de spot como un destino escalable mediante el comando register-scalable-target.
2. Cree una política de escalado mediante el comando put-scaling-policy.
3. Cree una alarma que active la política de escalado mediante el comando put-metric-alarm.

Escalado de la flota de spot mediante el escalado programado

El escalado según una programación le permite escalar la aplicación en respuesta a los cambios previstos en la demanda. Para utilizar el escalado programado, deberá crear acciones programadas que indican a la flota de spot que realice actividades de escalado en momentos específicos. Cuando crea una acción programada, especifica una flota de spot existente, cuándo debe ocurrir la actividad de escalado, la capacidad mínima y la capacidad máxima. Puede crear acciones programadas que realizan el escalado de forma puntual o periódica.

Solo puede crear una acción programada para la flotas de spot que ya exista. No puede crear una acción programada a la vez que crea una flota de spot.

Limitación

La solicitud de flota de spot debe tener un tipo de solicitud de `maintain`. El escalado automático no se admite para solicitudes de tipo `request` o bloques de spot.

Para crear una acción programada puntual

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

2. En el panel de navegación, elija Spot Requests (Solicitudes de spot).
3. Seleccione su solicitud de flota de spot y elija la pestaña Escalado programado cerca de la parte inferior de la pantalla.
4. Elija Crear acción programada.
5. En Nombre, especifique un nombre para la acción programada.
6. Escriba un valor para Capacidad mínima, Capacidad máxima o para ambas.
7. En Recurrencia, elija Una vez.
8. (Opcional) Elija una fecha y una hora para Hora de inicio, Hora de finalización o para ambas.
9. Elija Submit.

Para escalar de forma periódica

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Spot Requests (Solicitudes de spot).
3. Seleccione su solicitud de flota de spot y elija la pestaña Scheduled Scaling (Escalado programado) cerca de la parte inferior de la pantalla.
4. En Recurrencia, elija una de las programaciones predefinidas (por ejemplo, Todos los días) o elija Personalizada y escriba una expresión cron. Para obtener más información sobre las expresiones cron compatibles con el escalado programado, consulte Expresiones Cron en la Guía del usuario de Amazon CloudWatch Events.
5. (Opcional) Elija una fecha y una hora para Start time (Hora de inicio), End time (Hora de finalización) o para ambas.
6. Elija Submit.

Para editar una acción programada

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Spot Requests (Solicitudes de spot).
3. Seleccione su solicitud de flota de spot y elija la pestaña Scheduled Scaling (Escalado programado) cerca de la parte inferior de la pantalla.
4. Seleccione la acción programada y elija Acciones, Editar.
5. Introduzca los cambios necesarios y elija Enviar.

Para eliminar una acción programada

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Spot Requests (Solicitudes de spot).
3. Seleccione su solicitud de flota de spot y elija la pestaña Scheduled Scaling (Escalado programado) cerca de la parte inferior de la pantalla.
4. Seleccione la acción programada y elija Acciones, Eliminar.
5. Cuando se le pida confirmación, seleccione Delete (Eliminar).

Para administrar el escalado programado mediante la AWS CLI

Use los siguientes comandos:

- put-scheduled-action
- describe-scheduled-actions
- delete-scheduled-action

Monitorear los eventos de flotas con Amazon EventBridge

Cuando el estado de una flota de EC2 o de una flota de spot cambia, la flota emite una notificación. La notificación se pone a disposición como un evento que se envía a Amazon EventBridge (antes conocido como Amazon CloudWatch Events). Los eventos se emiten en la medida de lo posible.

Con Amazon EventBridge, puede crear reglas que desencadenen acciones programáticas en respuesta a un evento. Por ejemplo, puede crear dos reglas de EventBridge, una que se activa cuando cambia el estado de la flota y otra que se activa cuando se termina una instancia de la flota. Puede configurar la primera regla para que, si el estado de la flota cambia, la regla invoque un tema de SNS para enviarle una notificación por email. Puede configurar la segunda regla para que, si una instancia se termina, la regla invoque una función de Lambda para iniciar una nueva instancia.

Temas

- Tipos de eventos de flota de EC2
- Tipos de eventos de flota de spot
- Crear reglas de Amazon EventBridge

Tipos de eventos de flota de EC2

> **Note**
>
> Sólo las flotas de tipo `maintain` y `request` emiten eventos. Las flotas de tipo `instant` no emiten eventos porque envían solicitudes sincrónicas únicas y el estado de la flota se conoce inmediatamente en la respuesta.

Hay cinco tipos de eventos de flota de EC2. Para cada tipo de evento, hay varios subtipos.

Los eventos se envían a EventBridge en formato JSON. Los siguientes campos del evento forman el patrón de evento definido en la regla y que desencadena una acción:

`"source": "aws.ec2fleet"`

Identifica que el evento es de flota de EC2.

`"detail-type": "EC2 Fleet State Change"`

Identifica el tipo de evento.

`"detail": { "sub-type": "submitted" }`

Identifica el subtipo de evento.

Tipos de eventos

- Cambio de estado de flota EC2
- Cambio de solicitud de instancia de spot de flota EC2
- Cambio de instancia de flota de EC2
- Información sobre la flota EC2
- Error de flota EC2

Cambio de estado de flota EC2

La flota de EC2 envía un evento `EC2 Fleet State Change` a Amazon EventBridge cuando una flota de EC2 cambia el estado.

El siguiente es un ejemplo de los datos de este evento.

```
{
    "version": "0",
    "id": "715ed6b3-b8fc-27fe-fad6-528c7b8bf8a2",
    "detail-type": "EC2 Fleet State Change",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-11-09T09:00:20Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-598fb973-87b7-422d-
be4d-6b0809bfff0a"
    ],
    "detail": {
        "sub-type": "active"
    }
}
```

Los valores posibles de `sub-type` son:

`active`

La solicidud de flota de EC2 se ha validado y Amazon EC2 está intentando mantener el número de destino de instancias de ejecución.

`deleted`

La flota de EC2 solicitud se ha eliminado y no tiene ninguna instancia en ejecución. La flota de EC2 se elimina dos días después de que todas sus instancias se hayan terminado.

`deleted_running`

La Flota de EC2 solicitud se ha eliminado y no lanza instancias adicionales. Las instancias existentes de la flota continúan ejecutándose hasta que se interrumpen o terminan. La solicitud permanece en este estado hasta que se interrumpan o terminen todas las instancias.

`deleted_terminating`

La solicitud de flota de EC2 se ha eliminado y sus instancias están en proceso de terminación. La solicitud permanece en este estado hasta que se terminen todas las instancias.

`expired`

La solicitud de flota de EC2 ha caducado. Si la solicitud se creó con el conjunto de `TerminateInstancesWithExpiration`, un evento `terminated` posterior indica que las instancias han terminado.

`modify_in_progress`

La solicitud de flota de EC2 se está modificando. La solicitud permanece en este estado hasta que la modificación se procese completamente.

`modify_succeeded`

Se modificó la solicitud de flota de EC2.

`submitted`

La solicitud de flota de EC2 está en evaluación y Amazon EC2 se prepara para lanzar el número de instancias de destino.

`progress`

La solicitud de flota de EC2 está en proceso de cumplirse.

Cambio de solicitud de instancia de spot de flota EC2

La flota de EC2 envía un evento `EC2 Fleet Spot Instance Request Change` a Amazon EventBridge cuando una solicitud de instancia de spot en la flota cambia de estado.

El siguiente es un ejemplo de los datos de este evento.

```
{
    "version": "0",
    "id": "19331f74-bf4b-a3dd-0f1b-ddb1422032b9",
    "detail-type": "EC2 Fleet Spot Instance Request Change",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-11-09T09:00:05Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/
fleet-83fd4e48-552a-40ef-9532-82a3acca5f10"
    ],
    "detail": {
        "spot-instance-request-id": "sir-rmqske6h",
```

```
        "description": "SpotInstanceRequestId sir-rmqske6h, PreviousState:
 cancelled_running",
        "sub-type": "cancelled"
    }
}
```

Los valores posibles de `sub-type` son:

`active`

La solicitud de instancia de spot se ha completado y tiene una instancia de spot asociada.

`cancelled`

Ha cancelado la solicitud de instancia de spot o la solicitud de instancia de spot caducó.

`disabled`

Detuvo la instancia de spot.

`submitted`

Se ha enviado la solicitud de instancia de spot.

Cambio de instancia de flota de EC2

La flota de EC2 envía un evento `EC2 Fleet Instance Change` a Amazon EventBridge cuando una instancia de la flota cambia de estado.

El siguiente es un ejemplo de los datos de este evento.

```
{
    "version": "0",
    "id": "542ce428-c8f1-0608-c015-e8ed6522c5bc",
    "detail-type": "EC2 Fleet Instance Change",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-11-09T09:00:23Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-598fb973-87b7-422d-
be4d-6b0809bfff0a"
    ],
    "detail": {
        "instance-id": "i-0c594155dd5ff1829",
```

```
        "description": "{\"instanceType\":\"c5.large\",\"image\":\"ami-6057e21a\",
\"productDescription\":\"Linux/UNIX\",\"availabilityZone\":\"us-east-1d\"}",
        "sub-type": "launched"
    }
}
```

Los valores posibles de `sub-type` son:

`launched`

Se lanzó una nueva instancia.

`terminated`

La instancia se terminó.

`termination_notified`

Se envió una notificación de terminación de instancia cuando Amazon EC2 terminó una instancia de spot durante la reducción de escala, cuando la capacidad de destino de la flota se modificó hacia abajo; por ejemplo, de una capacidad de destino de 4 a una capacidad de destino de 3.

Información sobre la flota EC2

La flota de EC2 envía un evento `EC2 Fleet Information` a Amazon EventBridge cuando hay un error durante el cumplimiento. El evento de información no impide que la flota intente cumplir su capacidad de destino.

El siguiente es un ejemplo de los datos de este evento.

```
{
    "version": "0",
    "id": "76529817-d605-4571-7224-d36cc1b2c0c4",
    "detail-type": "EC2 Fleet Information",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-11-09T08:17:07Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-8becf5fe-
bb9e-415d-8f54-3fa5a8628b91"
    ],
    "detail": {
```

```
        "description": "c4.xlarge, ami-0947d2ba12ee1ff75, Linux/UNIX, us-east-1a,
 Spot price in either SpotFleetRequestConfigData or SpotFleetLaunchSpecification or
 LaunchTemplate or LaunchTemplateOverrides is less than Spot market price $0.0619",
        "sub-type": "launchSpecUnusable"
    }
}
```

Los valores posibles de `sub-type` son:

`fleetProgressHalted`

El precio de cada especificación de inicialización no es válido porque está por debajo del precio de spot (todas las especificaciones de inicialización han producido eventos `launchSpecUnusable`). Una especificación de inicialización podría volverse válida si cambia el precio de spot.

`launchSpecTemporarilyBlacklisted`

La configuración no es válida y varios intentos de iniciar instancias han fallado. Para obtener más información, consulte la descripción del evento.

`launchSpecUnusable`

El precio de una especificación de inicialización no es válido porque está por debajo del precio de spot.

`registerWithLoadBalancersFailed`

Error al intentar registrar instancias con equilibradores de carga. Para obtener más información, consulte la descripción del evento.

Error de flota EC2

La flota de EC2 envía un evento `EC2 Fleet Error` a Amazon EventBridge cuando hay un error durante el cumplimiento. El evento de error impide que la flota intente cumplir su capacidad de destino.

El siguiente es un ejemplo de los datos de este evento.

```
{
    "version": "0",
    "id": "69849a22-6d0f-d4ce-602b-b47c1c98240e",
    "detail-type": "EC2 Fleet Error",
```

```
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-10-07T01:44:24Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-9bb19bc6-60d3-4fd2-ae47-
d33e68eafa08"
    ],
    "detail": {
        "description": "m3.large, ami-00068cd7555f543d5, Linux/UNIX: IPv6 is not
 supported for the instance type 'm3.large'. ",
        "sub-type": "spotFleetRequestConfigurationInvalid"
    }
}
```

Los valores posibles de `sub-type` son:

`iamFleetRoleInvalid`

La flota de EC2 no tiene los permisos necesarios para iniciar o terminar una instancia.

`allLaunchSpecsTemporarilyBlacklisted`

Ninguna de las configuraciones es válida y varios intentos de iniciar instancias han fallado. Para obtener más información, consulte la descripción del evento.

`spotInstanceCountLimitExceeded`

Ha alcanzado el límite del número de instancias de spot que puede iniciar.

`spotFleetRequestConfigurationInvalid`

La configuración no es válida. Para obtener más información, consulte la descripción del evento.

Tipos de eventos de flota de spot

Hay cinco tipos de eventos de flota de spot. Para cada tipo de evento, hay varios subtipos.

Los eventos se envían a EventBridge en formato JSON. Los siguientes campos del evento forman el patrón de evento definido en la regla y que desencadena una acción:

`"source": "aws.ec2spotfleet"`

Identifica que el evento es de la flota de spot.

`"detail-type": "EC2 Spot Fleet State Change"`

Identifica el tipo de evento.

`"detail": { "sub-type": "submitted" }`

Identifica el subtipo de evento.

Tipos de eventos

- Cambio de estado de la flota de spot de EC2
- Cambio de solicitud de instancia de spot de flota de spot de EC2
- Cambio de instancia de flota de spot de EC2
- Información sobre la flota de spot de EC2
- Error de flota de spot de EC2

Cambio de estado de la flota de spot de EC2

La flota de spot envía un evento de `EC2 Spot Fleet State Change` a Amazon EventBridge cuando la flota de spot cambia de estado.

El siguiente es un ejemplo de los datos de este evento.

```
{
    "version": "0",
    "id": "d1af1091-6cc3-2e24-203a-3b870e455d5b",
    "detail-type": "EC2 Spot Fleet State Change",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-09T08:57:06Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-4b6d274d-0cea-4b2c-
b3be-9dc627ad1f55"
    ],
    "detail": {
        "sub-type": "submitted"
    }
}
```

Los valores posibles de `sub-type` son:

`active`

La solicitud de flota de spot se ha validado y Amazon EC2 está intentando mantener el número de destino de instancias de ejecución.

`cancelled`

La solicitud de flota de spot se ha cancelado y no tiene ninguna instancia de ejecución. La flota de spot se eliminará dos días después de que se terminen las instancias.

`cancelled_running`

La solicitud de flota de spot se ha cancelado y no inicia instancias adicionales. Las instancias existentes de la flota continúan ejecutándose hasta que se interrumpen o terminan. La solicitud permanece en este estado hasta que se interrumpan o terminen todas las instancias.

`cancelled_terminating`

La solicitud de flota de spot se ha cancelado y sus instancias están en proceso de terminación. La solicitud permanece en este estado hasta que se terminen todas las instancias.

`expired`

La solicitud de la flota de spot ha caducado. Si la solicitud se creó con el conjunto de `TerminateInstancesWithExpiration`, un evento `terminated` posterior indica que las instancias han terminado.

`modify_in_progress`

Se está modificando la solicitud de la flota de spot. La solicitud permanece en este estado hasta que la modificación se procese completamente.

`modify_succeeded`

Se modificó la solicitud de la flota de spot.

`submitted`

Se está evaluando la solicitud de la flota de spot y Amazon EC2 se está preparando para iniciar el número de instancias de destino.

`progress`

La solicitud de flota de spot está en proceso de cumplirse.

Cambio de solicitud de instancia de spot de flota de spot de EC2

La flota de spot envía un evento de `EC2 Spot Fleet Spot Instance Request Change` a Amazon EventBridge cuando una solicitud de instancia de spot en la flota cambia de estado.

El siguiente es un ejemplo de los datos de este evento.

```
{
    "version": "0",
    "id": "cd141ef0-14af-d670-a71d-fe46e9971bd2",
    "detail-type": "EC2 Spot Fleet Spot Instance Request Change",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-09T08:53:21Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-
a98d2133-941a-47dc-8b03-0f94c6852ad1"
    ],
    "detail": {
        "spot-instance-request-id": "sir-a2w9gc5h",
        "description": "SpotInstanceRequestId sir-a2w9gc5h, PreviousState:
 cancelled_running",
        "sub-type": "cancelled"
    }
}
```

Los valores posibles de `sub-type` son:

`active`

La solicitud de instancia de spot se ha completado y tiene una instancia de spot asociada.

`cancelled`

Ha cancelado la solicitud de instancia de spot o la solicitud de instancia de spot caducó.

`disabled`

Detuvo la instancia de spot.

`submitted`

Se ha enviado la solicitud de instancia de spot.

Cambio de instancia de flota de spot de EC2

La flota de spot envía un evento de `EC2 Spot Fleet Instance Change` a Amazon EventBridge cuando una instancia en la flota cambia de estado.

El siguiente es un ejemplo de los datos de este evento.

```
{
    "version": "0",
    "id": "11591686-5bd7-bbaa-eb40-d46529c2710f",
    "detail-type": "EC2 Spot Fleet Instance Change",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-09T07:25:02Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-c8a764a4-bedc-4b62-
af9c-0095e6e3ba61"
    ],
    "detail": {
        "instance-id": "i-08b90df1e09c30c9b",
        "description": "{\"instanceType\":\"r4.2xlarge\",\"image\":
\"ami-032930428bf1abbff\",\"productDescription\":\"Linux/UNIX\",\"availabilityZone\":
\"us-east-1a\"}",
        "sub-type": "launched"
    }
}
```

Los valores posibles de `sub-type` son:

`launched`

Se lanzó una nueva instancia.

`terminated`

La instancia se terminó.

`termination_notified`

Se envió una notificación de terminación de instancia cuando Amazon EC2 terminó una Instancia de spot durante la reducción de escala, cuando la capacidad de destino de la flota se modificó hacia abajo; por ejemplo, de una capacidad de destino de 4 a una capacidad de destino de 3.

Información sobre la flota de spot de EC2

La flota de spot envía un evento de `EC2 Spot Fleet Information` a Amazon EventBridge cuando hay un error durante el cumplimiento. El evento de información no impide que la flota intente cumplir su capacidad de destino.

El siguiente es un ejemplo de los datos de este evento.

```
{
    "version": "0",
    "id": "73a60f70-3409-a66c-635c-7f66c5f5b669",
    "detail-type": "EC2 Spot Fleet Information",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-08T20:56:12Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-2531ea06-
af18-4647-8757-7d69c94971b1"
    ],
    "detail": {
        "description": "r3.8xlarge, ami-032930428bf1abbff, Linux/UNIX, us-east-1a, Spot
 bid price is less than Spot market price $0.5291",
        "sub-type": "launchSpecUnusable"
    }
}
```

Los valores posibles de `sub-type` son:

`fleetProgressHalted`

El precio de cada especificación de inicialización no es válido porque está por debajo del precio de spot (todas las especificaciones de inicialización han producido eventos `launchSpecUnusable`). Una especificación de inicialización podría volverse válida si cambia el precio de spot.

`launchSpecTemporarilyBlacklisted`

La configuración no es válida y varios intentos de iniciar instancias han fallado. Para obtener más información, consulte la descripción del evento.

`launchSpecUnusable`

El precio de una especificación de inicialización no es válido porque está por debajo del precio de spot.

`registerWithLoadBalancersFailed`

Error al intentar registrar instancias con equilibradores de carga. Para obtener más información, consulte la descripción del evento.

Error de flota de spot de EC2

La flota de spot envía un evento de `EC2 Spot Fleet Error` a Amazon EventBridge cuando hay un error durante el cumplimiento. El evento de error impide que la flota intente cumplir su capacidad de destino.

El siguiente es un ejemplo de los datos de este evento.

```
{
    "version": "0",
    "id": "10adc4e7-675c-643e-125c-5bfa1b1ba5d2",
    "detail-type": "EC2 Spot Fleet Error",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-09T06:56:07Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/
sfr-38725d30-25f1-4f30-83ce-2907c56dba17"
    ],
    "detail": {
        "description": "r4.2xlarge, ami-032930428bf1abbff, Linux/UNIX: The
 associatePublicIPAddress parameter can only be specified for the network interface
 with DeviceIndex 0. ",
        "sub-type": "spotFleetRequestConfigurationInvalid"
    }
}
```

Los valores posibles de `sub-type` son:

`iamFleetRoleInvalid`

La flota de spot no tiene los permisos necesarios para iniciar o terminar una instancia.

`allLaunchSpecsTemporarilyBlacklisted`

Ninguna de las configuraciones es válida y varios intentos de iniciar instancias han fallado. Para obtener más información, consulte la descripción del evento.

`spotInstanceCountLimitExceeded`

Ha alcanzado el límite del número de instancias de spot que puede iniciar.

`spotFleetRequestConfigurationInvalid`

La configuración no es válida. Para obtener más información, consulte la descripción del evento.

Crear reglas de Amazon EventBridge

Cuando se emite una notificación de un cambio de estado para una flota de EC2 o una flota de spot, el evento de la notificación se envía a Amazon EventBridge. Si EventBridge detecta un patrón de eventos que coincide con un patrón definido en una regla, EventBridge invoca un destino (o destinos) especificados en la regla.

Puede escribir una regla de EventBridge y automatizar qué acciones tomar cuando el patrón de eventos coincida con la regla.

Temas

- Creación de reglas de Amazon EventBridge para monitorear eventos de flota de EC2
- Creación de reglas de Amazon EventBridge para monitorear eventos de flota de spot

Creación de reglas de Amazon EventBridge para monitorear eventos de flota de EC2

Cuando se emite una notificación de un cambio de estado para una flota de EC2, el evento de la notificación se envía a Amazon EventBridge en forma de un archivo JSON. Puede escribir una regla de EventBridge para automatizar qué acciones tomar cuando el patrón de eventos coincida con la regla. Si EventBridge detecta un patrón de eventos que coincide con un patrón definido en una regla, EventBridge invoca un destino (o destinos) especificado(s) en la regla.

Los siguientes campos forman el patrón de eventos definido en la regla:

`"source": "aws.ec2fleet"`

Identifica que el evento es de flota de EC2.

`"detail-type": "EC2 Fleet State Change"`

Identifica el tipo de evento.

`"detail": { "sub-type": "submitted" }`

Identifica el subtipo de evento.

Para obtener la lista de eventos de EC2 Fleet y datos de eventos de ejemplo, consulte the section called “Tipos de eventos de flota de EC2”.

Ejemplos

- Crear una regla de EventBridge para enviar una notificación
- Crear una regla de EventBridge para desencadenar una función de Lambda

Crear una regla de EventBridge para enviar una notificación

En el ejemplo siguiente se crea una regla de EventBridge para enviar un email, un mensaje de texto o una notificación push móvil cada vez que Amazon EC2 emite una notificación de cambio de estado de EC2 Fleet. La señal de este ejemplo se emite como un evento de `EC2 Fleet State Change`, lo que desencadena la acción definida por la regla.

Antes de crear la regla de EventBridge, debe crear el tema de Amazon SNS para el email, el mensaje de texto o la notificación push móvil.

Para crear una regla EventBridge para enviar una notificación cuando cambia el estado de una flota de EC2

1. Abra la consola de Amazon EventBridge en https://console.aws.amazon.com/events/.
2. Elija Crear regla.
3. En Definir detalle de la regla, haga lo siguiente:

   a. Ingrese un Nombre para la regla y, opcionalmente, una descripción.

      Una regla no puede tener el mismo nombre que otra regla de la misma región y del mismo bus de eventos.

   b. En Bus de eventos, elija Predeterminado. Cuando un servicio de AWS en su cuenta emite un evento, siempre se dirige al bus de eventos predeterminado de su cuenta.

   c. En Tipo de regla, elija Regla con un patrón de evento.

d. Elija Siguiente.

4. En Crear patrón de evento, realice una de las siguientes acciones:

   a. En Origen del evento, elija Eventos o eventos de socios de EventBridge de AWS.

   b. En Patrón del evento, en este ejemplo, especificará el siguiente patrón de evento para que coincida con el evento `EC2 Fleet Instance Change`.

```
{
 "source": ["aws.ec2fleet"],
 "detail-type": ["EC2 Fleet Instance Change"]
}
```

      Para agregar el patrón de evento, puede utilizar una plantilla por medio de la opción Formulario de patrón de evento o puede especificar su propio patrón por medio de la opción Patrón personalizado (editor de JSON), de la siguiente manera:

      i. Para utilizar una plantilla con el objetivo de crear el patrón de evento, haga lo siguiente:

         A. Seleccione Formulario de patrón de evento.

         B. En Origen del evento, elija Servicios de AWS.

         C. En Servicio de AWS, elija Flota de EC2.

         D. En Tipo de evento, elija Cambio de instancia de la flota de EC2.

         E. Para personalizar la plantilla, elija Editar patrón y realice los cambios para que coincidan con el patrón de evento de ejemplo.

      ii. (Alternativa) Para especificar un patrón de evento personalizado, haga lo siguiente:

         A. Elija Custom pattern (JSON editor) (Patrón personalizado [editor de JSON]).

         B. En el casillero Patrón de evento, agregue el patrón de eventos de este ejemplo.

   c. Elija Siguiente.

5. En Seleccionar destino, realice una de las siguientes acciones:

   a. En Tipos de destino, elija Servicio de AWS.

   b. En Seleccionar un destino, elija Tema de SNS para enviar un email, un mensaje de texto o una notificación push móvil cuando se produzca el evento.

   c. En Tema, elija un tema existente. Primero debe crear un tema de Amazon SNS mediante la consola de Amazon SNS. A fin de obtener más información, consulte Uso de Amazon SNS

para mensajería de aplicación a persona (A2P) en Guía para desarrolladores de Amazon Simple Notification Service.

d. (Opcional) En Configuración adicional, puede configurar opciones adicionales. Para obtener más información, consulte Creación de reglas de EventBridge que reaccionan a eventos (paso 16) en la Guía del usuario de Amazon EventBridge.

e. Elija Siguiente.

6. (Opcional) En Etiquetas, puede asignar una o varias etiquetas a la regla y, a continuación, elija Siguiente.

7. En Revisar y crear, realice una de las siguientes acciones:

   a. Revise los detalles de la regla y modifíquelos según sea necesario.

   b. Elija Crear regla.

Para obtener más información, consulte Reglas de Amazon EventBridge y Patrones de eventos de Amazon EventBridge en la Guía del usuario de Amazon EventBridge.

Crear una regla de EventBridge para desencadenar una función de Lambda

En el ejemplo siguiente se crea una regla de EventBridge para desencadenar una función de Lambda cada vez que Amazon EC2 emite una notificación de cambio de instancia de EC2 Fleet cuando se inicia una instancia. La señal de este ejemplo se emite como un evento de `EC2 Fleet Instance Change`, subtipo `launched`, lo que desencadena la acción definida por la regla.

Antes de crear la regla de EventBridge, debe crear la función de Lambda.

Para crear la función de Lambda que se utilizará en la regla de EventBridge

1. Abra la consola de AWS Lambda en https://console.aws.amazon.com/lambda/.

2. Elija Crear función.

3. Ingrese un nombre para su función, configure el código y luego elija Crear función.

   Para obtener más información sobre el uso de Lambda, consulte Crear una función de Lambda con la consola en la Guía para desarrolladores de AWS Lambda.

Para crear una regla EventBridge para activar una función de Lambda cuando cambia el estado de una instancia de una flota de EC2

1. Abra la consola de Amazon EventBridge en https://console.aws.amazon.com/events/.
2. Elija Crear regla.
3. En Definir detalle de la regla, haga lo siguiente:

   a. Ingrese un Nombre para la regla y, opcionalmente, una descripción.

      Una regla no puede tener el mismo nombre que otra regla de la misma región y del mismo bus de eventos.

   b. En Bus de eventos, elija Predeterminado. Cuando un servicio de AWS en su cuenta emite un evento, siempre se dirige al bus de eventos predeterminado de su cuenta.

   c. En Tipo de regla, elija Regla con un patrón de evento.

   d. Elija Siguiente.
4. En Crear patrón de evento, realice una de las siguientes acciones:

   a. En Origen del evento, elija Eventos o eventos de socios de EventBridge de AWS.

   b. En Patrón del evento, en este ejemplo, especificará el siguiente patrón de evento para que coincida con el evento `EC2 Fleet Instance Change` y el subtipo `launched`.

      ```
      {
       "source": ["aws.ec2fleet"],
       "detail-type": ["EC2 Fleet Instance Change"],
       "detail": {
         "sub-type": ["launched"]
      }
      ```

      Para agregar el patrón de evento, puede utilizar una plantilla por medio de la opción Formulario de patrón de evento o puede especificar su propio patrón por medio de la opción Patrón personalizado (editor de JSON), de la siguiente manera:

      i. Para utilizar una plantilla con el objetivo de crear el patrón de evento, haga lo siguiente:

         A. Seleccione Formulario de patrón de evento.

         B. En Origen del evento, elija Servicios de AWS.

         C. En Servicio de AWS, elija Flota de EC2.

D. En Event type (Tipo de evento), elija EC2 Fleet Instance Change (Cambio de instancia de la flota de EC2).

E. Elija Editar patrón y agregue `"detail": {"sub-type": ["launched"]` para que coincida con el patrón de evento de ejemplo. Para obtener el formato JSON adecuado, inserte una coma (`,`) después del corchete anterior (`]`).

ii. (Alternativa) Para especificar un patrón de evento personalizado, haga lo siguiente:

A. Elija Custom pattern (JSON editor) (Patrón personalizado [editor de JSON]).

B. En el casillero Patrón de evento, agregue el patrón de eventos de este ejemplo.

c. Elija Siguiente.

5. En Seleccionar destino, realice una de las siguientes acciones:

a. En Tipos de destino, elija Servicio de AWS.

b. En Seleccionar un destino, elija Tema de SNS para enviar un email, un mensaje de texto o una notificación push móvil cuando se produzca el evento.

c. En Tema, elija Función de Lambda y en Función, elija la función que creó para responder cuando se produzca el evento.

d. (Opcional) En Configuración adicional, puede configurar opciones adicionales. Para obtener más información, consulte Creación de reglas de EventBridge que reaccionan a eventos (paso 16) en la Guía del usuario de Amazon EventBridge.

e. Elija Siguiente.

6. (Opcional) En Etiquetas, puede asignar una o varias etiquetas a la regla y, a continuación, elija Siguiente.

7. En Revisar y crear, realice una de las siguientes acciones:

a. Revise los detalles de la regla y modifíquelos según sea necesario.

b. Elija Crear regla.

Para obtener un tutorial sobre cómo crear una función de Lambda y una regla de EventBridge que ejecute la función de Lambda, consulte Tutorial: registrar el estado de una instancia de Amazon EC2 mediante EventBridge en la Guía para desarrolladores de AWS Lambda.

Creación de reglas de Amazon EventBridge para monitorear eventos de flota de spot

Cuando se emite una notificación de un cambio de estado para una flota de spot, el evento de la notificación se envía a Amazon EventBridge en forma de un archivo JSON. Puede escribir una regla de EventBridge para automatizar qué acciones tomar cuando el patrón de eventos coincida con la regla. Si EventBridge detecta un patrón de eventos que coincide con un patrón definido en una regla, EventBridge invoca un destino (o destinos) especificado(s) en la regla.

Los siguientes campos forman el patrón de eventos definido en la regla:

`"source": "aws.ec2spotfleet"`

Identifica que el evento es de la flota de spot.

`"detail-type": "EC2 Spot Fleet State Change"`

Identifica el tipo de evento.

`"detail": { "sub-type": "submitted" }`

Identifica el subtipo de evento.

Para obtener la lista de eventos de la flota de spot y datos de eventos de ejemplo, consulte the section called “Tipos de eventos de flota de spot”.

Ejemplos

- Crear una regla de EventBridge para enviar una notificación
- Crear una regla de EventBridge para desencadenar una función de Lambda

Crear una regla de EventBridge para enviar una notificación

En el ejemplo siguiente se crea una regla de EventBridge para enviar un email, un mensaje de texto o una notificación push móvil cada vez que Amazon EC2 emite una notificación de cambio de estado de la flota de spot. La señal de este ejemplo se emite como un evento de `EC2 Spot Fleet State Change`, lo que desencadena la acción definida por la regla. Antes de crear la regla de EventBridge, debe crear el tema de Amazon SNS para el email, el mensaje de texto o la notificación push móvil.

Para crear una regla de EventBridge a fin de enviar una notificación cuando el estado de la flota de spot cambia

1. Abra la consola de Amazon EventBridge en https://console.aws.amazon.com/events/.

2. Elija Crear regla.
3. En Definir detalle de la regla, haga lo siguiente:
   a. Ingrese un Nombre para la regla y, opcionalmente, una descripción.

      Una regla no puede tener el mismo nombre que otra regla de la misma región y del mismo bus de eventos.
   b. En Bus de eventos, elija Predeterminado. Cuando un servicio de AWS en su cuenta emite un evento, siempre se dirige al bus de eventos predeterminado de su cuenta.
   c. En Tipo de regla, elija Regla con un patrón de evento.
   d. Elija Siguiente.
4. En Crear patrón de evento, realice una de las siguientes acciones:
   a. En Origen del evento, elija Eventos o eventos de socios de EventBridge de AWS.
   b. En Patrón del evento, en este ejemplo, especificará el siguiente patrón de evento para que coincida con el evento `EC2 Spot Fleet Instance Change`.

      ```
      {
       "source": ["aws.ec2spotfleet"],
       "detail-type": ["EC2 Spot Fleet Instance Change"]
      }
      ```

      Para agregar el patrón de evento, puede utilizar una plantilla por medio de la opción Formulario de patrón de evento o puede especificar su propio patrón por medio de la opción Patrón personalizado (editor de JSON), de la siguiente manera:

      i. Para utilizar una plantilla con el objetivo de crear el patrón de evento, haga lo siguiente:

         A. Seleccione Formulario de patrón de evento.

         B. En Origen del evento, elija Servicios de AWS.

         C. En Servicio de AWS, elija Flota de spot de EC2.

         D. En Tipo de evento, elija Cambio de instancia de la flota de spot de EC2.

         E. Para personalizar la plantilla, elija Editar patrón y realice los cambios para que coincidan con el patrón de evento de ejemplo.

      ii. (Alternativa) Para especificar un patrón de evento personalizado, haga lo siguiente:

         A. Elija Custom pattern (JSON editor) (Patrón personalizado [editor de JSON]).

B. En el casillero Patrón de evento, agregue el patrón de eventos de este ejemplo.

c. Elija Siguiente.

5. En Seleccionar destino, realice una de las siguientes acciones:

   a. En Tipos de destino, elija Servicio de AWS.

   b. En Seleccionar un destino, elija Tema de SNS para enviar un email, un mensaje de texto o una notificación push móvil cuando se produzca el evento.

   c. En Tema, elija un tema existente. Primero debe crear un tema de Amazon SNS mediante la consola de Amazon SNS. A fin de obtener más información, consulte Uso de Amazon SNS para mensajería de aplicación a persona (A2P) en Guía para desarrolladores de Amazon Simple Notification Service.

   d. (Opcional) En Configuración adicional, puede configurar opciones adicionales. Para obtener más información, consulte Creación de reglas de EventBridge que reaccionan a eventos (paso 16) en la Guía del usuario de Amazon EventBridge.

   e. Elija Siguiente.

6. (Opcional) En Etiquetas, puede asignar una o varias etiquetas a la regla y, a continuación, elija Siguiente.

7. En Revisar y crear, realice una de las siguientes acciones:

   a. Revise los detalles de la regla y modifíquelos según sea necesario.

   b. Elija Crear regla.

Para obtener más información, consulte Reglas de Amazon EventBridge y Patrones de eventos de Amazon EventBridge en la Guía del usuario de Amazon EventBridge.

Crear una regla de EventBridge para desencadenar una función de Lambda

En el ejemplo siguiente se crea una regla de EventBridge para desencadenar una función de Lambda cada vez que Amazon EC2 emite una notificación de cambio de instancia de la flota de spot. La señal de este ejemplo se emite como un evento de `EC2 Spot Fleet Instance Change`, subtipo `launched`, lo que desencadena la acción definida por la regla.

Antes de crear la regla de EventBridge, debe crear la función de Lambda.

Para crear la función de Lambda que se utilizará en la regla de EventBridge

1. Abra la consola de AWS Lambda en https://console.aws.amazon.com/lambda/.

2. Elija Crear función.
3. Ingrese un nombre para su función, configure el código y luego elija Crear función.

   Para obtener más información sobre el uso de Lambda, consulte Crear una función de Lambda con la consola en la Guía para desarrolladores de AWS Lambda.

Para crear una regla EventBridge a fin de desencadenar una función de Lambda cuando una instancia de una flota de spot cambia de estado

1. Abra la consola de Amazon EventBridge en https://console.aws.amazon.com/events/.
2. Elija Crear regla.
3. En Definir detalle de la regla, haga lo siguiente:

   a. Ingrese un Nombre para la regla y, opcionalmente, una descripción.

      Una regla no puede tener el mismo nombre que otra regla de la misma región y del mismo bus de eventos.

   b. En Bus de eventos, elija Predeterminado. Cuando un servicio de AWS en su cuenta emite un evento, siempre se dirige al bus de eventos predeterminado de su cuenta.

   c. En Tipo de regla, elija Regla con un patrón de evento.

   d. Elija Siguiente.
4. En Crear patrón de evento, realice una de las siguientes acciones:

   a. En Origen del evento, elija Eventos o eventos de socios de EventBridge de AWS.

   b. En Patrón del evento, en este ejemplo, especificará el siguiente patrón de evento para que coincida con el evento `EC2 Spot Fleet Instance Change` y el subtipo `launched`.

```
{
 "source": ["aws.ec2spotfleet"],
 "detail-type": ["EC2 Spot Fleet Instance Change"],
 "detail": {
   "sub-type": ["launched"]
}
```

   Para agregar el patrón de evento, puede utilizar una plantilla por medio de la opción Formulario de patrón de evento o puede especificar su propio patrón por medio de la opción Patrón personalizado (editor de JSON), de la siguiente manera:

i. Para utilizar una plantilla con el objetivo de crear el patrón de evento, haga lo siguiente:

A. Seleccione Formulario de patrón de evento.

B. En Origen del evento, elija Servicios de AWS.

C. En Servicio de AWS, elija Flota de spot de EC2.

D. En Event type (Tipo de evento), elija EC2 Spot Fleet Instance Change (Cambio de instancia de la flota de spot de EC2).

E. Elija Edit pattern (Editar patrón) y agregue `"detail": {"sub-type": ["launched"]` para que coincida con el patrón de evento de ejemplo. Para obtener el formato JSON adecuado, inserte una coma (`,`) después del corchete anterior (`]`).

ii. (Alternativa) Para especificar un patrón de evento personalizado, haga lo siguiente:

A. Elija Custom pattern (JSON editor) (Patrón personalizado [editor de JSON]).

B. En el casillero Patrón de evento, agregue el patrón de eventos de este ejemplo.

c. Elija Siguiente.

5. En Seleccionar destino, realice una de las siguientes acciones:

a. En Tipos de destino, elija Servicio de AWS.

b. En Seleccionar un destino, elija Tema de SNS para enviar un email, un mensaje de texto o una notificación push móvil cuando se produzca el evento.

c. En Tema, elija Función de Lambda y en Función, elija la función que creó para responder cuando se produzca el evento.

d. (Opcional) En Configuración adicional, puede configurar opciones adicionales. Para obtener más información, consulte Creación de reglas de EventBridge que reaccionan a eventos (paso 16) en la Guía del usuario de Amazon EventBridge.

e. Elija Siguiente.

6. (Opcional) En Etiquetas, puede asignar una o varias etiquetas a la regla y, a continuación, elija Siguiente.

7. En Revisar y crear, realice una de las siguientes acciones:

a. Revise los detalles de la regla y modifíquelos según sea necesario.

b. Elija Crear regla.

Para obtener un tutorial sobre cómo crear una función de Lambda y una regla de EventBridge que ejecute la función de Lambda, consulte Tutorial: registrar el estado de una instancia de Amazon EC2 mediante EventBridge en la Guía para desarrolladores de AWS Lambda.

Tutoriales para la flota de EC2 y flota de spot

Los siguientes tutoriales lo guiarán por los procesos comunes para crear flotas de EC2 y flotas de spot.

Tutoriales

- Tutorial: Uso de flota de EC2 con ponderación de instancias
- Tutorial: Uso de flota de EC2 con la capacidad en diferido como modelo principal
- Tutorial: Inicialización de instancias bajo demanda con reservas de capacidad específicas
- Tutorial: Inicialización de instancias en bloques de capacidad
- Tutorial: Utiliza la flota de spot con ponderación de instancias

Tutorial: Uso de flota de EC2 con ponderación de instancias

Este tutorial utiliza una compañía ficticia llamada Example Corp para ilustrar el proceso de solicitud de una flota de EC2 mediante la ponderación de instancias.

Objetivo

Example Corp es una compañía farmacéutica que desea usar la potencia computacional de Amazon EC2 para realizar el cribado de compuestos químicos que podrían utilizarse para combatir el cáncer.

Planificación

Example Corp primero consulta las Prácticas recomendadas para instancias de spot. A continuación, Example Corp determina los siguientes requisitos para la flota de EC2.

Tipos de instancias

Example Corp tiene una aplicación que requiere un uso intensivo de memoria y de recursos informáticos que responde mejor con 60 GB de memoria, como mínimo, y ocho CPU virtuales (vCPU). Desean maximizar estos recursos para la aplicación al precio más bajo posible. Example Corp decide que cualquiera de los siguientes tipos de instancias EC2 podría satisfacer sus necesidades:

Tipo de instancia	Memoria (GiB)	vCPU
r3.2xlarge	61	8
r3.4xlarge	122	16
r3.8xlarge	244	32

Capacidad de destino en unidades

Con ponderación de instancias, la capacidad de destino puede ser igual a un número de instancias (opción predeterminada) o a una combinación de factores como núcleos (vCPU), memoria (GiB) y almacenamiento (GB). Considerando la base para su aplicación (60 GB de RAM y ocho vCPU) como una unidad, Example Corp decide que 20 veces esta cantidad satisfaría sus necesidades. Así que la compañía establece la capacidad de destino de la solicitud de flota de EC2 en 20.

Ponderaciones de instancias

Después de determinar la capacidad de destino, Example Corp calcula las ponderaciones de instancias. Para calcularlas para cada tipo de instancia, determinan las unidades de cada tipo de instancia que son necesarias para alcanzar la capacidad de destino de la siguiente manera:

- r3.2xlarge (61,0 GB, 8 vCPU) = 1 unidad de 20
- r3.4xlarge (122,0 GB, 16 vCPU) = 2 unidades de 20
- r3.8xlarge (244,0 GB, 32 vCPU) = 4 unidades de 20

Por consiguiente, Example Corp asigna ponderaciones de instancias de 1, 2 y 4 a las respectivas configuraciones de inicialización en la solicitud de flota de EC2.

Precio por hora de unidad

Example Corp usa el precio bajo demanda por hora de instancia como punto de inicio de su precio. También podrían usar precios de spot recientes o una combinación de ambos. Para calcular el precio por hora de unidad, dividen el precio inicial por hora de instancia entre la ponderación. Por ejemplo:

Tipo de instancia	Precio bajo demanda	Ponderación de instancia	Precio por hora de unidad
r3.2xLarge	0,7 USD	1	0,7 USD
r3.4xLarge	1,4 USD	2	0,7 USD
r3.8xLarge	2,8 USD	4	0,7 USD

Example Corp podría usar un precio global por hora de unidad de 0,7 USD y ser competitivos para los tres tipos de instancias. También podrían usar un precio global por hora de unidad de 0,7 USD y un precio específico por hora de unidad de 0,9 USD en la especificación de inicialización `r3.8xlarge`.

Verificar permisos

Antes de crear una flota de EC2, Example Corp comprueba que tiene un rol de IAM con los permisos necesarios. Para obtener más información, consulte Requisitos previos de flota de EC2.

Crear una plantilla de lanzamiento

A continuación, Example Corp crea una plantilla de inicialización. El ID de la plantilla de inicio se utiliza en el paso siguiente. Para obtener más información, consulte Creación de una plantilla de lanzamiento.

Crear la flota de EC2

Example Corp crea un archivo, `config.json`, con la siguiente configuración para su flota de EC2. En el ejemplo siguiente, reemplace los identificadores de recursos por sus propios identificadores de recursos.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-07b3bc7625cdab851",
                "Version": "1"
```

```
            },
            "Overrides": [
                {
                    "InstanceType": "r3.2xlarge",
                    "SubnetId": "subnet-482e4972",
                    "WeightedCapacity": 1
                },
                {
                    "InstanceType": "r3.4xlarge",
                    "SubnetId": "subnet-482e4972",
                    "WeightedCapacity": 2
                },
                {
                    "InstanceType": "r3.8xlarge",
                    "MaxPrice": "0.90",
                    "SubnetId": "subnet-482e4972",
                    "WeightedCapacity": 4
                }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    }
}
```

Example Corp crea la solicitud de flota de EC2 con el siguiente comando create-fleet.

```
aws ec2 create-fleet \
    --cli-input-json file://config.json
```

Para obtener más información, consulte Crear una flota de EC2.

Cumplimiento

La estrategia de asignación determina de qué grupos de capacidad de spot proceden las instancias de spot.

Con la estrategia `lowest-price` (que es la estrategia predeterminada), las instancias de spot proceden del grupo con el precio de spot más bajo por unidad en el momento de la prestación del servicio. Para proporcionar 20 unidades de capacidad, la flota de EC2 inicia 20 (20 dividido entre 1)

instancias `r3.2xlarge`, 10 (20 dividido ente 2) instancias `r3.4xlarge` o 5 (20 dividido entre 4) instancias `r3.8xlarge`.

Si Example Corp usara la estrategia `diversified`, las instancias de spot procederían de los tres grupos. La flota de EC2 iniciaría 6 instancias `r3.2xlarge` (que proporcionan 6 unidades), 3 instancias `r3.4xlarge` (que proporcionan 6 unidades) y 2 instancias `r3.8xlarge` (que proporcionan 8 unidades), con un total de 20 unidades.

Tutorial: Uso de flota de EC2 con la capacidad en diferido como modelo principal

En este tutorial, se utiliza una compañía ficticia llamada ABC Online para ilustrar el proceso de solicitud de una flota de EC2 que usa la capacidad en diferido como modelo principal y la capacidad de spot en caso de estar disponible.

Objetivo

ABC Online, una compañía de telerestaurante, desea poder aprovisionar la capacidad de Amazon EC2 con diversos tipos de instancias EC2 y opciones de compra con el fin de alcanzar sus objetivos de escala, rendimiento y costo.

Plan

ABC Online requiere una cantidad de capacidad fija para operar durante los periodos de actividad punta, pero desearía beneficiarse de aumentarla a un precio más bajo. ABC Online determina los siguientes requisitos para su flota de EC2:

- Capacidad de instancias bajo demanda: ABC Online requiere 15 instancias bajo demanda para asegurarse de poder cubrir el tráfico de los periodos de actividad máxima.
- Capacidad de instancias de spot: ABC Online desearía mejorar el rendimiento, pero a un precio más bajo, mediante el aprovisionamiento de 5 instancias de spot.

Verificar permisos

Antes de crear una flota de EC2, ABC Online comprueba que tiene un rol de IAM con los permisos necesarios. Para obtener más información, consulte Requisitos previos de flota de EC2.

Crear una plantilla de lanzamiento

A continuación, ABC Online crea una plantilla de inicialización. El ID de la plantilla de inicio se utiliza en el paso siguiente. Para obtener más información, consulte Creación de una plantilla de lanzamiento.

Crear la flota de EC2

ABC Online crea un archivo, `config.json`, con la siguiente configuración para su flota de EC2. En el ejemplo siguiente, reemplace los identificadores de recursos por sus propios identificadores de recursos.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-07b3bc7625cdab851",
                "Version": "2"
            }

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "OnDemandTargetCapacity":15,
        "DefaultTargetCapacityType": "spot"
    }
}
```

ABC Online crea la flota de EC2 con el siguiente comando create-fleet.

```
aws ec2 create-fleet \
    --cli-input-json file://config.json
```

Para obtener más información, consulte Crear una flota de EC2.

Cumplimiento

La estrategia de asignación determina que la capacidad bajo demanda se atienda siempre, mientras que el resto de la capacidad de destino se cubre con instancias de spot si hay capacidad y disponibilidad.

Tutorial: Inicialización de instancias bajo demanda con reservas de capacidad específicas

En este tutorial se explican todos los pasos que debe realizar para que su flota de EC2 lance instancias bajo demanda en reservas de capacidad `targeted`.

Aprenderá a configurar una flota para utilizar primero las reservas de capacidad bajo demanda `targeted` al iniciar instancias bajo demanda. También aprenderá a configurar la flota para que, cuando la capacidad total de destino bajo demanda supere el número de reservas de capacidad sin utilizar disponibles, la flota utilice la estrategia de asignación especificada a fin de seleccionar los grupos de instancias en los que iniciará la capacidad de destino restante.

Configuración de la flota de EC2

En este tutorial, la configuración de la flota es la siguiente:

- Capacidad de destino: 10 instancias bajo demanda
- Total de reservas de capacidad `targeted` sin utilizar: 6 (menos que la capacidad de destino bajo demanda de 10 instancias bajo demanda de la flota)
- Número de grupos de reservas de capacidad: 2 (`us-east-1a` y `us-east-1b`)
- Número de reservas de capacidad por grupo: 3
- Estrategia de asignación bajo demanda: `lowest-price` (cuando el número de reservas de capacidad sin utilizar es menor que la capacidad de destino bajo demanda, la flota determina los grupos en los que iniciará la capacidad bajo demanda restante en función de la estrategia de asignación bajo demanda).

  Tenga en cuenta que también puede utilizar la estrategia de asignación `prioritized` en lugar de la `lowest-price`.

Para iniciar instancias bajo demanda en reservas de capacidad targeted, debe realizar una serie de pasos, como se indica a continuación:

- Paso 1: crear reservas de capacidad
- Paso 2: crear un grupo de recursos de reserva de capacidad
- Paso 3: agregar las reservas de capacidad al grupo de recursos de reserva de capacidad
- (Opcional) Paso 4: ver las reservas de capacidad en el grupo de recursos

- Paso 5: crear una plantilla de inicialización que especifique que la reserva de capacidad se dirige a un grupo de recursos específico
- (Opcional) Paso 6: describir la plantilla de inicialización
- Paso 7: crear una flota de EC2
- (Opcional) Paso 8: ver el número de reservas de capacidad sin utilizar restantes

Paso 1: crear reservas de capacidad

Utilice el comando create-capacity-reservation a fin de crear las reservas de capacidad, tres para `us-east-1a` y otras tres para `us-east-1b`. Excepto por la zona de disponibilidad, los demás atributos de las reservas de capacidad son idénticos.

3 reservas de capacidad en **`us-east-1a`**

```
aws ec2 create-capacity-reservation \
    --availability-zone us-east-1a\
    --instance-type c5.xlarge\
    --instance-platform Linux/UNIX \
    --instance-count 3 \
    --instance-match-criteria targeted
```

Ejemplo del ID de reserva de capacidad resultante

```
cr-1234567890abcdef1
```

3 reservas de capacidad en **`us-east-1b`**

```
aws ec2 create-capacity-reservation \
    --availability-zone us-east-1b\
    --instance-type c5.xlarge\
    --instance-platform Linux/UNIX \
    --instance-count 3 \
    --instance-match-criteria targeted
```

Ejemplo del ID de reserva de capacidad resultante

```
cr-54321abcdef567890
```

Paso 2: crear un grupo de recursos de reserva de capacidad

Utilice el servicio `resource-groups` y el comando create-group para crear un grupo de recursos de reserva de capacidad. En este ejemplo, el grupo de recursos se llama `my-cr-group`. Para obtener información sobre por qué debe crear un grupo de recursos, consulte Utilizar reservas de capacidad para instancias bajo demanda.

```
aws resource-groups create-group \
    --name my-cr-group \
    --configuration '{"Type":"AWS::EC2::CapacityReservationPool"}'
 '{"Type":"AWS::ResourceGroups::Generic", "Parameters": [{"Name": "allowed-resource-
types", "Values": ["AWS::EC2::CapacityReservation"]}]}'
```

Paso 3: agregar las reservas de capacidad al grupo de recursos de reserva de capacidad

Utilice el servicio `resource-groups` y el comando group-resources para agregar las reservas de capacidad que creó en el paso 1 al grupo de recursos de reserva de capacidad. Tenga en cuenta que debe hacer referencia a las reservas de capacidad bajo demanda por sus ARN.

```
aws resource-groups group-resources \
    --group my-cr-group \
    --resource-arns \
      arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1 \
      arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-54321abcdef567890
```

Ejemplo de resultado

```
{
   "Failed": [],
   "Succeeded": [
   "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1",
   "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-54321abcdef567890"
   ]
}
```

(Opcional) Paso 4: ver las reservas de capacidad en el grupo de recursos

Utilice el servicio `resource-groups` y el comando list-group-resources para describir opcionalmente el grupo de recursos y ver sus reservas de capacidad.

```
aws resource-groups list-group-resources --group my-cr-group
```

Ejemplo de resultado

```
{
    "ResourceIdentifiers": [
        {
            "ResourceType": "AWS::EC2::CapacityReservation",
            "ResourceArn": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/
cr-1234567890abcdef1"
        },
        {
            "ResourceType": "AWS::EC2::CapacityReservation",
            "ResourceArn": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/
cr-54321abcdef567890"
        }
    ]
}
```

Paso 5: crear una plantilla de inicialización que especifique que la reserva de capacidad se dirige a un grupo de recursos específico

Utilice el comando create-launch-template para crear una plantilla de inicialización en la que se especificarán las reservas de capacidad que se utilizarán. En este ejemplo, la flota utilizará reservas de capacidad `targeted`, que se han agregado a un grupo de recursos. Por lo tanto, los datos de la plantilla de inicialización especifican que la reserva de capacidad se dirige a un grupo de recursos específico. En este ejemplo, la plantilla de inicialización se llama `my-launch-template`.

```
aws ec2 create-launch-template \
    --launch-template-name my-launch-template \
    --launch-template-data \
        '{"ImageId": "ami-0123456789example",
          "CapacityReservationSpecification":
            {"CapacityReservationTarget":
                { "CapacityReservationResourceGroupArn": "arn:aws:resource-groups:us-
east-1:123456789012:group/my-cr-group" }
            }
        }'
```

(Opcional) Paso 6: describir la plantilla de inicialización

Utilice el comando describe-launch-template para describir opcionalmente la plantilla de inicialización y ver su configuración.

```
aws ec2 describe-launch-template-versions --launch-template-name my-launch-template
```

Ejemplo de resultado

```
{
    "LaunchTemplateVersions": [
        {
            "LaunchTemplateId": "lt-01234567890example",
            "LaunchTemplateName": "my-launch-template",
            "VersionNumber": 1,
            "CreateTime": "2021-01-19T20:50:19.000Z",
            "CreatedBy": "arn:aws:iam::123456789012:user/Admin",
            "DefaultVersion": true,
            "LaunchTemplateData": {
                "ImageId": "ami-0947d2ba12ee1ff75",
                "CapacityReservationSpecification": {
                    "CapacityReservationTarget": {
                        "CapacityReservationResourceGroupArn": "arn:aws:resource-
groups:us-east-1:123456789012:group/my-cr-group"
                    }
                }
            }
        }
    ]
}
```

Paso 7: crear una flota de EC2

Cree una flota de EC2 que especifique la información de configuración de las instancias que iniciará. La siguiente configuración de flota de EC2 solo muestra las configuraciones pertinentes para este ejemplo. La plantilla de inicialización `my-launch-template` es la plantilla de inicialización que creó en el paso 5. Hay dos grupos de instancias, cada uno con el mismo tipo de instancias (`c5.xlarge`), pero con diferentes zonas de disponibilidad (`us-east-1a` y `us-east-1b`). El precio de los grupos de instancias es el mismo porque los precios se definen para la región, no por zona de disponibilidad. La capacidad total de destino es de 10 y el tipo de capacidad de destino predeterminado es on-

demand. La estrategia de asignación bajo demanda es `lowest-price`. La estrategia de uso para las reservas de capacidad es `use-capacity-reservations-first`.

> **Note**
>
> El tipo de flota debe ser `instant`. Otros tipos de flotas no admiten `use-capacity-reservations-first`.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
            "Overrides": [
               {
                   "InstanceType": "c5.xlarge",
                   "AvailabilityZone": "us-east-1a"
               },
               {
                    "InstanceType": "c5.xlarge",
                    "AvailabilityZone": "us-east-1b"
               }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 10,
        "DefaultTargetCapacityType": "on-demand"
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price",
        "CapacityReservationOptions": {
             "UsageStrategy": "use-capacity-reservations-first"
         }
    },
    "Type": "instant"
}
```

Después de crear la flota `instant` con la configuración anterior, se inician las siguientes 10 instancias para cumplir con la capacidad de destino:

- Las reservas de capacidad se utilizan en primer lugar para iniciar 6 instancias bajo demanda de la siguiente manera:
  - 3 instancias bajo demanda se lanzan en las 3 reservas de capacidad `targeted` `c5.xlarge` en `us-east-1a`
  - 3 instancias bajo demanda se lanzan en las 3 reservas de capacidad `targeted` `c5.xlarge` en `us-east-1b`
- Para alcanzar la capacidad de destino, se inician 4 instancias bajo demanda adicionales en la capacidad bajo demanda normal de acuerdo con la estrategia de asignación bajo demanda, que es `lowest-price` en este ejemplo. Sin embargo, dado que los grupos tienen el mismo precio (porque el precio es por región y no por zona de disponibilidad), la flota inicia las 4 instancias bajo demanda restantes en cualquiera de los grupos.

(Opcional) Paso 8: ver el número de reservas de capacidad sin utilizar restantes

Después de iniciar la flota, opcionalmente puede ejecutar describe-capacity-reservations para ver cuántas reservas de capacidad sin utilizar quedan. En este ejemplo, debería ver la siguiente respuesta, que muestra que se utilizaron todas las reservas de capacidad de todos los grupos.

```
{ "CapacityReservationId":  "cr-111",
     "InstanceType":  "c5.xlarge",
     "AvailableInstanceCount":  0
}

 { "CapacityReservationId":  "cr-222",
     "InstanceType":  "c5.xlarge",
     "AvailableInstanceCount":  0
}
```

Tutorial: Inicialización de instancias en bloques de capacidad

En este tutorial se explican los pasos que debe seguir para que su flota de EC2 lance instancias en bloques de capacidad. Para obtener más información acerca de los bloques de capacidad, consulte bloques de capacidad para ML.

Puede utilizar una flota de EC2 de tipo instantáneo para iniciar instancias en bloques de capacidad. Para obtener más información, consulte Utilizar una flota de EC2 de tipo “instantáneo”.

En la mayoría de los casos, la capacidad de destino de la solicitud de flota de EC2 debe ser menor o igual que la capacidad disponible de la reserva de bloques de capacidad a la que se dirige. No se atenderán las solicitudes de capacidad de destino que superen los límites de la reserva de bloques de capacidad. Si la solicitud de capacidad de destino supera los límites de su reserva de bloques de capacidad, se mostrará una excepción de capacidad insuficiente para la capacidad que supere los límites de su reserva de bloques de capacidad.

> **Note**
>
> En el caso de bloques de capacidad, la flota de EC2 no recurrirá a la inicialización de instancias bajo demanda en el resto de la capacidad de destino deseada.

Si flota de EC2 no puede cumplir con la capacidad de destino solicitada en una reserva de bloques de capacidad disponible, la flota de EC2 ocupará toda la capacidad posible y devolverá las instancias que haya podido iniciar. Puede repetir la llamada a la flota de EC2 de nuevo hasta que se hayan aprovisionado todas las instancias.

Tras configurar la solicitud de la flota de EC2, debe esperar hasta la fecha de inicio de la reserva de bloques de capacidad. Si hace solicitudes a la flota de EC2 para iniciar un bloque de capacidad que aún no se ha iniciado, se mostrará un error de capacidad insuficiente.

Una vez que se active su reserva de bloques de capacidad, podrá hacer llamadas a la API de la flota de EC2 y aprovisionar las instancias en su bloque de capacidad en función de los parámetros que haya seleccionado. Las instancias que se ejecutan en el bloque de capacidad seguirán ejecutándose hasta que las detenga o termine mediante una llamada a la API de Amazon EC2 independiente o hasta que Amazon EC2 termine las instancias cuando finalice la reserva de bloques de capacidad.

Consideraciones

- No se admiten varios bloques de capacidad en la misma solicitud `CreateFleet`.
- No se admite el uso de `OnDemandTargetCapacity` ni `SpotTargetCapacity` al mismo tiempo que el valor de `capacity-block` esté establecido en `DefaultTargetCapacity`.
- Si el valor de `DefaultTargetCapacityType` está establecido en `capacity-block`, no puede proporcionar `OnDemandOptions::CapacityReservationOptions`. Se producirá una excepción.

Creación de una plantilla de lanzamiento

El ID de la plantilla de inicio se utiliza en el paso siguiente. Para obtener más información, consulte Creación de una plantilla de lanzamiento.

Para configurar la plantilla de inicialización para `InstanceMarketOptionsRequest`, establezca `MarketType` en `capacity-block`. Especifique el ID de reserva de bloques de capacidad al que se dirige; para ello, establezca el parámetro `CapacityReservationID`.

Crear la flota de EC2

Cree un archivo, `config.json`, con la siguiente configuración para su flota de EC2. En el ejemplo siguiente, reemplace los identificadores de recursos por sus propios identificadores de recursos.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "CBR-launch-template",
                "Version": "1"
            },
            "Overrides": [
                {
                    "InstanceType": "p5.48xlarge",
                    "AvailabilityZone": "us-east-1a"
                },
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 10,
        "DefaultTargetCapacityType": "capacity-block"
    },
    "Type": "instant"
}
```

Utilice el siguiente comando create-fleet.

```
aws ec2 create-fleet \
     --cli-input-json file://config.json
```

Para obtener más información, consulte Crear una flota de EC2.

Tutorial: Utiliza la flota de spot con ponderación de instancias

Este tutorial utiliza una empresa ficticia llamada Example Corp para ilustrar el proceso de solicitud de una flota de spot mediante la ponderación de instancias.

Objetivo

Example Corp es una compañía farmacéutica que desea aprovechar la potencia computacional de Amazon EC2 para realizar el cribado de compuestos químicos que podrían utilizarse para combatir el cáncer.

Planificación

Example Corp primero consulta las Prácticas recomendadas para instancias de spot. A continuación, Example Corp determina los siguientes requisitos para su flota de spot.

Tipos de instancias

Example Corp tiene una aplicación que requiere un uso intensivo de memoria y de recursos informáticos que responde mejor con 60 GB de memoria, como mínimo, y ocho CPU virtuales (vCPU). Desean maximizar estos recursos para la aplicación al precio más bajo posible. Example Corp decide que cualquiera de los siguientes tipos de instancias EC2 podría satisfacer sus necesidades:

Tipo de instancia	Memoria (GiB)	vCPU
r3.2xlarge	61	8
r3.4xlarge	122	16
r3.8xlarge	244	32

Capacidad de destino en unidades

Con ponderación de instancias, la capacidad de destino puede ser igual a un número de instancias (opción predeterminada) o a una combinación de factores como núcleos (vCPU), memoria (GiB) y almacenamiento (GB). Considerando la base para su aplicación (60 GB de RAM y ocho vCPU) como 1 unidad, Example Corp decide que 20 veces esta cantidad satisfaría sus necesidades. Así que la compañía establece la capacidad de destino de la solicitud de flota de spot en 20.

Ponderaciones de instancias

Después de determinar la capacidad de destino, Example Corp calcula las ponderaciones de instancias. Para calcularlas para cada tipo de instancia, determinan las unidades de cada tipo de instancia que son necesarias para alcanzar la capacidad de destino de la siguiente manera:

- r3.2xlarge (61,0 GB, 8 vCPU) = 1 unidad de 20
- r3.4xlarge (122,0 GB, 16 vCPU) = 2 unidades de 20
- r3.8xlarge (244,0 GB, 32 vCPU) = 4 unidades de 20

Por consiguiente, Example Corp asigna ponderaciones de instancias de 1, 2 y 4 a las respectivas configuraciones de inicialización en la solicitud de flota de spot.

Precio por hora de unidad

Example Corp usa el precio bajo demanda por hora de instancia como punto de inicio de su precio. También podrían usar precios de spot recientes o una combinación de ambos. Para calcular el precio por hora de unidad, dividen el precio inicial por hora de instancia entre la ponderación. Por ejemplo:

Tipo de instancia	Precio bajo demanda	Ponderación de instancia	Precio por hora de unidad
r3.2xLarge	0,7 USD	1	0,7 USD
r3.4xLarge	1,4 USD	2	0,7 USD
r3.8xLarge	2,8 USD	4	0,7 USD

Example Corp podría usar un precio global por hora de unidad de 0,7 USD y ser competitivos para los tres tipos de instancias. También podrían usar un precio global por hora de unidad de 0,7 USD y un precio específico por hora de unidad de 0,9 USD en la especificación de inicialización `r3.8xlarge`.

Verificar permisos

Antes de crear una solicitud de flota de spot, Example Corp verifica que tiene un rol de IAM con los permisos necesarios. Para obtener más información, consulte Permisos de flota de spot.

Crear la solicitud

Example Corp crea un archivo, `config.json`, con la siguiente configuración para su solicitud de flota de spot:

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
    {
      "ImageId": "ami-1a2b3c4d",
      "InstanceType": "r3.2xlarge",
      "SubnetId": "subnet-482e4972",
      "WeightedCapacity": 1
    },
    {
      "ImageId": "ami-1a2b3c4d",
      "InstanceType": "r3.4xlarge",
      "SubnetId": "subnet-482e4972",
      "WeightedCapacity": 2
    },
    {
      "ImageId": "ami-1a2b3c4d",
      "InstanceType": "r3.8xlarge",
      "SubnetId": "subnet-482e4972",
      "SpotPrice": "0.90",
      "WeightedCapacity": 4
    }
  ]
}
```

Example Corp crea la solicitud de flota de spot con el comando request-spot-fleet.

```
aws ec2 request-spot-fleet --spot-fleet-request-config file://config.json
```

Para obtener más información, consulte Tipos de solicitudes de flota de spot.

Cumplimiento

La estrategia de asignación determina de qué grupos de capacidad de spot proceden las instancias de spot.

Con la estrategia `lowestPrice` (que es la estrategia predeterminada), las instancias de spot proceden del grupo con el precio de spot más bajo por unidad en el momento de la prestación del servicio. Para proporcionar 20 unidades de capacidad, la flota de spot inicia 20 instancias `r3.2xlarge` (20 dividido por 1), 10 instancias `r3.4xlarge` (20 dividido por 2) o 5 instancias `r3.8xlarge` (20 dividido por 4).

Si Example Corp usara la estrategia `diversified`, las instancias de spot procederían de los tres grupos. La flota de spot iniciaría 6 instancias `r3.2xlarge` (que proporcionan 6 unidades), 3 instancias `r3.4xlarge` (que proporcionan 6 unidades) y 2 instancias `r3.8xlarge` (que proporcionan 8 unidades), con un total de 20 unidades.

Configuraciones de ejemplo para la flota de EC2 y la flota de spot

En los siguientes ejemplos, se muestran configuraciones de inicialización que puede utilizar para crear flotas de EC2 y flotas de spot.

Temas

Configuraciones de ejemplo de flota de EC2

En los siguientes ejemplos, se muestran configuraciones de inicialización que puede utilizar con el comando create-fleet para crear una flota de EC2. Para obtener más información acerca de los parámetros, consulte create-fleet en la Referencia de comandos de la AWS CLI.

Ejemplos

- Ejemplo 9: lanzamiento de instancias de spot en una flota de capacidad optimizada con prioridades
- Ejemplo 10: inicialización de instancias de spot en una flota price-capacity-optimized
- Ejemplo 11: configuración de la selección de tipos de instancias basada en atributos

Ejemplo 1: inicialización de instancias de spot como opción de compra predeterminada

En el ejemplo siguiente se especifican los parámetros mínimos que se requieren en una flota de EC2: una plantilla de lanzamiento, la capacidad de destino y la opción de compra predeterminada. La plantilla de inicialización se identifica mediante su ID y número de versión. La capacidad de destino de la flota es de dos instancias y la opción de compra predeterminado es `spot`, lo que da lugar a que la flota lance dos instancias de spot.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            }

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 2,
        "DefaultTargetCapacityType": "spot"
    }
}
```

Ejemplo 2: inicialización de instancias bajo demanda como opción de compra predeterminada

En el ejemplo siguiente se especifican los parámetros mínimos que se requieren en una flota de EC2: una plantilla de lanzamiento, la capacidad de destino y la opción de compra predeterminada. La plantilla de lanzamiento se identifica mediante su ID y número de versión. La capacidad de destino de la flota es de dos instancias y la opción de compra predeterminado es `on-demand`, lo que da lugar a que la flota lance dos instancias bajo demanda.

```
{
    "LaunchTemplateConfigs": [
```

```
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            }

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 2,
        "DefaultTargetCapacityType": "on-demand"
    }
}
```

Ejemplo 3: inicialización de instancias bajo demanda como opción de capacidad principal

En el siguiente ejemplo se especifica una capacidad de destino total de 2 instancias para la flota y una capacidad de destino de 1 instancia a petición. La opción de compra predeterminada es `spot`. La flota inicia 1 instancia a petición según lo especificado, pero ha de iniciar otra instancia más para cubrir la capacidad de destino total. La opción de compra aplicada a la diferencia se calcula de la siguiente manera: `TotalTargetCapacity` – `OnDemandTargetCapacity` = `DefaultTargetCapacityType`, lo que da lugar a que la flota lance una instancia de spot.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            }

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 2,
        "OnDemandTargetCapacity": 1,
        "DefaultTargetCapacityType": "spot"
    }
}
```

Ejemplo 4: inicialización de instancias bajo demanda con varias reservas de capacidad

Puede configurar una flota para usar Reservas de capacidad bajo demanda primero al lanzar Instancias bajo demanda estableciendo la estrategia de uso para Reservas de capacidad en `use-capacity-reservations-first`. En este ejemplo se muestra cómo la flota selecciona las reservas de capacidad que se utilizarán cuando hay más reservas de capacidad de las que se necesitan para cumplir con la capacidad de destino.

En este ejemplo, la configuración de flota es la siguiente:

- Capacidad de destino: 12 instancias bajo demanda
- Total de reservas de capacidad sin utilizar: 15 (más que la capacidad de destino de 12 instancias bajo demanda de la flota)
- Número de grupos de reservas de capacidad: 3 (`m5.large`, `m4.xlarge` y `m4.2xlarge`)
- Número de reservas de capacidad por grupo: 5
- Estrategia de asignación bajo demanda: `lowest-price` (cuando hay varias reservas de capacidad sin utilizar en varios grupos de instancias, la flota determina los grupos en los que se iniciarán las instancias bajo demanda en función de la estrategia de asignación bajo demanda).

  Tenga en cuenta que también puede utilizar la estrategia de asignación `prioritized` en lugar de la `lowest-price`.

Reservas de capacidad

La cuenta tiene las siguientes 15 reservas de capacidad sin utilizar en 3 grupos diferentes. El número de Reservas de capacidad en cada grupo se indica por `AvailableInstanceCount`.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-222",
```

```
    "InstanceType": "m4.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount":5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

Configuración de flota

La siguiente configuración de flota solo muestra las configuraciones pertinentes para este ejemplo. La capacidad total de destino es 12 y el tipo de capacidad de destino predeterminado es `on-demand`. La estrategia de asignación bajo demanda es `lowest-price`. La estrategia de uso para las reservas de capacidad es `use-capacity-reservations-first`.

En este ejemplo, el precio de instancia bajo demanda es:

- `m5.large`: 0,096 USD por hora
- `m4.xlarge`: 0,20 USD por hora
- `m4.2xlarge`: 0,40 USD por hora

> **Note**
>
> El tipo de flota debe ser `instant`. Otros tipos de flotas no admiten `use-capacity-reservations-first`.

```
{
    "LaunchTemplateConfigs": [
```

```
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-abc1234567example",
                "Version": "1"
            }
            "Overrides": [
                {
                  "InstanceType": "m5.large",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                },
                {
                  "InstanceType": "m4.xlarge",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                },
                {
                  "InstanceType": "m4.2xlarge",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                }
              ]

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 12,
        "DefaultTargetCapacityType": "on-demand"
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price"
        "CapacityReservationOptions": {
            "UsageStrategy": "use-capacity-reservations-first"
        }
    },
    "Type": "instant",
}
```

Después de crear la flota `instant` con la configuración anterior, se inician las siguientes 12 instancias para cumplir con la capacidad de destino:

- 5 instancias bajo demanda `m5.large` en `us-east-1a`: `m5.large` en `us-east-1a` es el precio más bajo y hay 5 reservas de capacidad `m5.large` sin utilizar disponibles

- 5 instancias bajo demanda `m4.xlarge` en us-east-1a: `m4.xlarge` en `us-east-1a` es el siguiente precio más bajo y hay 5 reservas de capacidad `m4.xlarge` sin utilizar disponibles
- 2 instancias bajo demanda `m4.2xlarge` en us-east-1a: `m4.2xlarge` en `us-east-1a` es el tercer precio más bajo y hay 5 reservas de capacidad `m4.2xlarge` sin utilizar disponibles, de las cuales solo 2 son necesarias para satisfacer la capacidad de destino

Después de lanzar la flota, puede ejecutar describe-capacity-reservations para ver cuántas reservas de capacidad sin utilizar quedan. En este ejemplo, debería ver la siguiente respuesta, que muestra que se utilizaron todas las reservas de capacidad `m5.large` y `m4.xlarge`, y quedan 3 reservas de capacidad `m4.2xlarge` sin utilizar.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "m4.xlarge",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
    "AvailableInstanceCount": 3
}
```

Ejemplo 5: inicialización de instancias bajo demanda con reservas de capacidad cuando la capacidad total de destino supera el número de reservas de capacidad sin utilizar

Puede configurar una flota para usar Reservas de capacidad bajo demanda primero al lanzar Instancias bajo demanda estableciendo la estrategia de uso para Reservas de capacidad en `use-capacity-reservations-first`. En este ejemplo se muestra cómo la flota selecciona los grupos de instancias en los que se iniciarán las instancias bajo demanda cuando la capacidad total de destino supera el número de reservas de capacidad sin utilizar disponibles.

En este ejemplo, la configuración de flota es la siguiente:

- Capacidad de destino: 16 instancias bajo demanda
- Total de reservas de capacidad sin utilizar: 15 (menos que la capacidad de destino de 16 instancias bajo demanda de la flota)
- Número de grupos de reservas de capacidad: 3 (`m5.large`, `m4.xlarge` y `m4.2xlarge`)
- Número de reservas de capacidad por grupo: 5
- Estrategia de asignación bajo demanda: `lowest-price` (cuando el número de reservas de capacidad sin utilizar es menor que la capacidad de destino bajo demanda, la flota determina los grupos en los que lanzará la capacidad bajo demanda restante en función de la estrategia de asignación bajo demanda).

  Tenga en cuenta que también puede utilizar la estrategia de asignación `prioritized` en lugar de la `lowest-price`.

Reservas de capacidad

La cuenta tiene las siguientes 15 reservas de capacidad sin utilizar en 3 grupos diferentes. El número de Reservas de capacidad en cada grupo se indica por `AvailableInstanceCount`.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "m4.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

```
{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount":5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

Configuración de flota

La siguiente configuración de flota solo muestra las configuraciones pertinentes para este ejemplo. La capacidad total de destino es 16 y el tipo de capacidad de destino predeterminado es `on-demand`. La estrategia de asignación bajo demanda es `lowest-price`. La estrategia de uso para las reservas de capacidad es `use-capacity-reservations-first`.

En este ejemplo, el precio de instancia bajo demanda es:

- m5.large – 0,096 USD por hora
- m4.xlarge – 0,20 USD por hora
- m4.2xlarge: 0,40 USD por hora

> **Note**
>
> El tipo de flota debe ser `instant`. Otros tipos de flotas no admiten `use-capacity-reservations-first`.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            }
            "Overrides": [
                {
                  "InstanceType": "m5.large",
```

```
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                },
                {
                  "InstanceType": "m4.xlarge",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                },
                {
                  "InstanceType": "m4.2xlarge",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                }
              ]

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 16,
        "DefaultTargetCapacityType": "on-demand"
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price"
        "CapacityReservationOptions": {
            "UsageStrategy": "use-capacity-reservations-first"
        }
    },
    "Type": "instant",
}
```

Después de crear la flota `instant` con la configuración anterior, se inician las siguientes 16 instancias para satisfacer la capacidad de destino:

- 6 instancias bajo demanda `m5.large` en `us-east-1a`: `m5.large` en `us-east-1a` es el precio más bajo y hay 5 reservas de capacidad `m5.large` sin utilizar disponibles. Las reservas de capacidad se utilizan en primer lugar para iniciar 5 instancias bajo demanda. Luego de que se utilicen las reservas de capacidad `m4.xlarge` y `m4.2xlarge` restantes, se inicia una instancia bajo demanda adicional de acuerdo con la estrategia de asignación bajo demanda, que es `lowest-price` en este ejemplo, para alcanzar la capacidad de destino.
- 5 instancias bajo demanda `m4.xlarge` en `us-east-1a`: `m4.xlarge` en `us-east-1a` es el siguiente precio más bajo y hay 5 reservas de capacidad `m4.xlarge` sin utilizar disponibles

- 5 instancias bajo demanda `m4.2xlarge` en `us-east-1a`: `m4.2xlarge` en `us-east-1a` es el tercer precio más bajo y hay 5 reservas de capacidad `m4.2xlarge` sin utilizar disponibles

Después de lanzar la flota, puede ejecutar describe-capacity-reservations para ver cuántas reservas de capacidad sin utilizar quedan. En este ejemplo, debería ver la siguiente respuesta, que muestra que se utilizaron todas las reservas de capacidad de todos los grupos.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "m4.xlarge",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
    "AvailableInstanceCount": 0
}
```

Ejemplo 6: inicialización de instancias bajo demanda con reservas de capacidad específicas

Puede configurar una flota a fin de que utilice primero reservas de capacidad bajo demanda `targeted` al iniciar instancias bajo demanda al establecer la estrategia de uso para las reservas de capacidad en `use-capacity-reservations-first`. En este ejemplo se muestra cómo iniciar instancias bajo demanda en reservas de capacidad `targeted`, donde los atributos de las reservas de capacidad son los mismos, excepto por sus zonas de disponibilidad (`us-east-1a` y `us-east-1b`). También se muestra cómo la flota selecciona los grupos de instancias en los que se iniciarán las instancias bajo demanda cuando la capacidad total de destino supera el número de reservas de capacidad sin utilizar disponibles.

En este ejemplo, la configuración de flota es la siguiente:

- Capacidad de destino: 10 instancias bajo demanda

- Total de reservas de capacidad `targeted` sin utilizar: 6 (menos que la capacidad de destino bajo demanda de 10 instancias bajo demanda de la flota)
- Número de grupos de reservas de capacidad: 2 (`us-east-1a` y `us-east-1b`)
- Número de reservas de capacidad por grupo: 3
- Estrategia de asignación bajo demanda: `lowest-price` (cuando el número de reservas de capacidad sin utilizar es menor que la capacidad de destino bajo demanda, la flota determina los grupos en los que iniciará la capacidad bajo demanda restante en función de la estrategia de asignación bajo demanda).

  Tenga en cuenta que también puede utilizar la estrategia de asignación `prioritized` en lugar de la `lowest-price`.

Para obtener una explicación de los procedimientos que debe realizar para llevar a cabo este ejemplo, consulte Tutorial: Inicialización de instancias bajo demanda con reservas de capacidad específicas.

Reservas de capacidad

La cuenta tiene las siguientes 6 reservas de capacidad sin utilizar en 2 grupos diferentes. En este ejemplo, los grupos difieren en las zonas de disponibilidad. El número de Reservas de capacidad en cada grupo se indica por `AvailableInstanceCount`.


```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "c5.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 3,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c5.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1b",
    "AvailableInstanceCount": 3,
    "InstanceMatchCriteria": "open",
    "State": "active"
```

```
}
```

Configuración de flota

La siguiente configuración de flota solo muestra las configuraciones pertinentes para este ejemplo. La capacidad total de destino es de 10 y el tipo de capacidad de destino predeterminado es `on-demand`. La estrategia de asignación bajo demanda es `lowest-price`. La estrategia de uso para las reservas de capacidad es `use-capacity-reservations-first`.

En este ejemplo, el precio de la instancia bajo demanda para `c5.xlarge` en `us-east-1` es 0,17 USD por hora.

> **Note**
>
> El tipo de flota debe ser `instant`. Otros tipos de flotas no admiten `use-capacity-reservations-first`.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
            "Overrides": [
               {
                   "InstanceType": "c5.xlarge",
                   "AvailabilityZone": "us-east-1a"
               },
               {
                    "InstanceType": "c5.xlarge",
                    "AvailabilityZone": "us-east-1b"
               }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 10,
        "DefaultTargetCapacityType": "on-demand"
    },
```

```
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price",
        "CapacityReservationOptions": {
             "UsageStrategy": "use-capacity-reservations-first"
         }
    },
    "Type": "instant"
}
```

Después de crear la flota `instant` con la configuración anterior, se inician las siguientes 10 instancias para cumplir con la capacidad de destino:

- Las reservas de capacidad se utilizan en primer lugar para iniciar 6 instancias bajo demanda de la siguiente manera:
  - 3 instancias bajo demanda se lanzan en las 3 reservas de capacidad `targeted` `c5.xlarge` en `us-east-1a`
  - 3 instancias bajo demanda se lanzan en las 3 reservas de capacidad `targeted` `c5.xlarge` en `us-east-1b`
- Para alcanzar la capacidad de destino, se inician 4 instancias bajo demanda adicionales en la capacidad bajo demanda normal de acuerdo con la estrategia de asignación bajo demanda, que es `lowest-price` en este ejemplo. Sin embargo, dado que los grupos tienen el mismo precio (porque el precio es por región y no por zona de disponibilidad), la flota lanza las 4 instancias bajo demanda restantes en cualquiera de los grupos.

Después de lanzar la flota, puede ejecutar describe-capacity-reservations para ver cuántas reservas de capacidad sin utilizar quedan. En este ejemplo, debería ver la siguiente respuesta, que muestra que se utilizaron todas las reservas de capacidad de todos los grupos.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "c5.xlarge",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c5.xlarge",
    "AvailableInstanceCount": 0
}
```

Ejemplo 7: configuración del reequilibrio de capacidad para iniciar instancias de spot de reemplazo

En el siguiente ejemplo, se configura la flota de EC2 para iniciar una instancia de spot de reemplazo cuando Amazon EC2 emite una recomendación de reequilibrio para una instancia de spot en su flota. Para configurar el reemplazo automático de Instancias de spot para `ReplacementStrategy`, especifique `launch-before-terminate`. Para configurar el retraso de tiempo desde que se inician las nuevas instancias de spot de reemplazo hasta que se eliminan automáticamente las instancias de spot anteriores, especifique en `termination-delay` un valor en segundos. Para obtener más información, consulte Opciones de configuración.

> **Note**
>
> Recomendamos utilizar `launch-before-terminate` solo si puede predecir cuánto tardarán en completarse los procedimientos de cierre de instancias, de modo que las instancias anteriores solo terminen una vez que se hayan completado estos procedimientos. Se cobrará por todas las instancias mientras se ejecutan.

La efectividad de la estrategia de reequilibrio de capacidad depende del número de grupos de capacidades de spot especificadas en la solicitud de flota de EC2. Se recomienda configurar la flota con un conjunto diversificado de tipos de instancia y zonas de disponibilidad y para `AllocationStrategy`especificar `capacity-optimized`. Para obtener más información acerca de lo que debe tener en cuenta al configurar una flota de EC2 para reequilibrio de la capacidad, consulte Reequilibrio de la capacidad.

```
{
    "ExcessCapacityTerminationPolicy": "termination",
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "LaunchTemplate",
                "Version": "1"
            },
                 "Overrides": [
                       {
                           "InstanceType": "c3.large",
                           "WeightedCapacity": 1,
                            "Placement": {
```

```
                            "AvailabilityZone": "us-east-1a"
                        }
                    },
                    {
                        "InstanceType": "c4.large",
                        "WeightedCapacity": 1,
                         "Placement": {
                            "AvailabilityZone": "us-east-1a"
                        }
                    },
                    {
                        "InstanceType": "c5.large",
                        "WeightedCapacity": 1,
                         "Placement": {
                            "AvailabilityZone": "us-east-1a"
                        }
                    }
                ]
          }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 5,
        "DefaultTargetCapacityType": "spot"
    },
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "MaintenanceStrategies": {
            "CapacityRebalance": {
                "ReplacementStrategy": "launch-before-terminate",
                "TerminationDelay": "720"
            }
        }
    }
}
```

Ejemplo 8: inicialización de instancias de spot en una flota de capacidad optimizada

En el siguiente ejemplo se demuestra el modo de configurar una flota de EC2 con una estrategia de asignación de spot que optimiza la capacidad. Para optimizar la capacidad, debe establecer `AllocationStrategy` en `capacity-optimized`.

En el siguiente ejemplo, las tres especificaciones de lanzamiento determinan tres grupos de capacidad de spot. La capacidad de destino es de 50 instancias de spot. La flota de EC2 intenta

iniciar 50 instancias de spot en el grupo de capacidad de spot con capacidad óptima para el número de instancias que va a iniciar.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
                 "Overrides": [
                       {
                           "InstanceType": "r4.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2a"
                           },
                      },
                       {
                           "InstanceType": "m4.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2b"
                           },
                       },
                       {
                           "InstanceType": "c5.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2b"
                           }
                       }
                  ]
           }
    ],
    "TargetCapacitySpecification": {
            "TotalTargetCapacity": 50,
            "DefaultTargetCapacityType": "spot"

    }
}
```

Ejemplo 9: lanzamiento de instancias de spot en una flota de capacidad optimizada con prioridades

En el siguiente ejemplo se demuestra el modo de configurar una flota de EC2 con una estrategia de asignación de spot que optimiza la capacidad mientras utiliza la prioridad sobre la base del mejor esfuerzo.

Cuando se utiliza la estrategia de asignación `capacity-optimized-prioritized`, puede utilizar el parámetro `Priority` para especificar las prioridades de los grupos de capacidad de spot, donde cuanto menor es el número, mayor es la prioridad. También puede establecer la misma prioridad para varios grupos de capacidad de spot si los prefiere por igual. Si no establece una prioridad para un grupo, este se considerará último en términos de prioridad.

Para priorizar los grupos de capacidad de spot, debe establecer `AllocationStrategy` en `capacity-optimized-prioritized`. La flota de EC2 optimizará la capacidad en primer lugar, pero respetará las prioridades sobre la base del mejor esfuerzo (por ejemplo, si respetar las prioridades no afecta significativamente la capacidad de la flota de EC2 para aprovisionar capacidad óptima). Esta es una buena opción para cargas de trabajo en las que se debe minimizar la posibilidad de interrupción y también importa la preferencia por ciertos tipos de instancias.

En el siguiente ejemplo, las tres especificaciones de lanzamiento determinan tres grupos de capacidad de spot. Cada grupo se prioriza, de manera que cuanto menor sea el número, mayor es la prioridad. La capacidad de destino es de 50 instancias de spot. La flota de EC2 intenta iniciar 50 instancias de spot en el grupo de capacidad de spot con la máxima prioridad sobre la base del mejor esfuerzo, pero optimiza primero la capacidad.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized-prioritized"
        },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
                 "Overrides": [
                        {
                           "InstanceType": "r4.2xlarge",
                           "Priority": 1,
                           "Placement": {
```

```
                            "AvailabilityZone": "us-west-2a"
                        },
                    },
                     {
                        "InstanceType": "m4.2xlarge",
                        "Priority": 2,
                        "Placement": {
                            "AvailabilityZone": "us-west-2b"
                        },
                     },
                     {
                        "InstanceType": "c5.2xlarge",
                        "Priority": 3,
                        "Placement": {
                            "AvailabilityZone": "us-west-2b"
                        }
                     }
                ]
            }
    ],
    "TargetCapacitySpecification": {
            "TotalTargetCapacity": 50,
            "DefaultTargetCapacityType": "spot"
}
```

Ejemplo 10: inicialización de instancias de spot en una flota price-capacity-optimized

En el siguiente ejemplo, se muestra cómo configurar una flota de EC2 con una estrategia de asignación de spot que optimiza tanto para la capacidad como para el precio más bajo. Para optimizar la capacidad, además de tener en cuenta el precio, debe establecer el elemento `AllocationStrategy` de spot en `price-capacity-optimized`.

En el siguiente ejemplo, las tres especificaciones de lanzamiento determinan tres grupos de capacidad de spot. La capacidad de destino es de 50 instancias de spot. La flota de EC2 intenta iniciar 50 instancias de spot en el grupo de capacidad de spot con capacidad óptima para la cantidad de instancias que se van a iniciar y, al mismo tiempo, elegir el grupo que tenga el precio más bajo.

```
{
    "SpotOptions": {
        "AllocationStrategy": "price-capacity-optimized",
        "MinTargetCapacity": 2,
        "SingleInstanceType": true
```

```
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price"
    },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
                 "Overrides": [
                       {
                           "InstanceType": "r4.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2a"
                           },
                      },
                       {
                           "InstanceType": "m4.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2b"
                           },
                       },
                       {
                           "InstanceType": "c5.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2b"
                           }
                       }
                  ]
           }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 50,
        "OnDemandTargetCapacity":0,
        "SpotTargetCapacity":50,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Ejemplo 11: configuración de la selección de tipos de instancias basada en atributos

En el siguiente ejemplo, se muestra cómo configurar una flota de EC2 para utilizar la selección de tipos de instancia basada en atributos para identificar los tipos de instancia. Para especificar los atributos de instancia necesarios, especifique los atributos en la estructura de `InstanceRequirements`.

En el siguiente ejemplo, se especifican dos atributos de instancia:

- `VCpuCount`: se especifica un mínimo de 2 vCPU. Como no se especifica ningún máximo, no hay ningún límite máximo.
- `MemoryMiB`: se especifica un mínimo de 4 MiB de memoria. Como no se especifica ningún máximo, no hay ningún límite máximo.

Se identificarán los tipos de instancia que tengan 2 o más vCPU y 4 MiB o más de memoria. Sin embargo, la protección de precios y la estrategia de asignación pueden excluir algunos tipos de instancia cuando la flota de EC2 aprovisiona la flota.

Para obtener una lista y descripciones de todos los atributos posibles que se pueden especificar, consulte InstanceRequirements en la Referencia de la API de Amazon EC2.

```
{
 "SpotOptions": {
  "AllocationStrategy": "price-capacity-optimized"
 },
 "LaunchTemplateConfigs": [{
  "LaunchTemplateSpecification": {
   "LaunchTemplateName": "my-launch-template",
   "Version": "1"
  },
  "Overrides": [{
   "InstanceRequirements": {
    "VCpuCount": {
     "Min": 2
    },
    "MemoryMiB": {
     "Min": 4
    }
   }
  }]
 }],
```

```
 "TargetCapacitySpecification": {
  "TotalTargetCapacity": 20,
  "DefaultTargetCapacityType": "spot"
 },
 "Type": "instant"
}
```

Configuraciones de ejemplo de flota de spot

En los siguientes ejemplos, se muestran configuraciones de inicialización que puede utilizar con el comando request-spot-fleet para crear una solicitud de flota de spot. Para obtener más información, consulte Creación de una solicitud de flota de spot.

> **Note**
>
> En la flota de spot, no se puede indicar un ID de interfaz de red en una especificación de inicialización. No olvide omitir el parámetro `NetworkInterfaceID` en la plantilla o especificación de inicialización.

Ejemplos

- Ejemplo 1: inicialización de instancias de spot con la zona de disponibilidad o subred de menor precio de la región
- Ejemplo 2: inicialización de instancias de spot con la zona de disponibilidad o subred de menor precio de una lista especificada
- Ejemplo 3: inicialización de instancias de spot con el tipo de instancia de menor precio de una lista especificada
- Ejemplo 4. Anulación del precio para la solicitud
- Ejemplo 5: inicialización de una flota de spot con la estrategia de asignación diversificada
- Ejemplo 6: inicialización de una flota de spot con ponderación de instancias
- Ejemplo 7: inicialización de una flota de spot con capacidad bajo demanda
- Ejemplo 8: configurar el reequilibrio de capacidad para lanzar el reemplazo Instancias de spot
- Ejemplo 9: lanzamiento de instancias de spot en una flota de capacidad optimizada
- Ejemplo 10: lanzamiento de instancias de spot en una flota de capacidad optimizada con prioridades
- Ejemplo 11: inicialización de instancias de spot en una flota priceCapacityOptimized

- Ejemplo 12: configuración de la selección de tipos de instancia basada en atributos

Ejemplo 1: inicialización de instancias de spot con la zona de disponibilidad o subred de menor precio de la región

En el siguiente ejemplo se describe una especificación de inicialización sin una zona de disponibilidad o una subred. La flota de spot inicia las instancias en la zona de disponibilidad de menor precio que tenga una subred predeterminada. El precio que paga no supera el precio bajo demanda.

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "KeyName": "my-key-pair",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "m3.medium",
          "IamInstanceProfile": {
              "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
          }
      }
  ]
}
```

Ejemplo 2: inicialización de instancias de spot con la zona de disponibilidad o subred de menor precio de una lista especificada

En los siguientes ejemplos se describen dos especificaciones de inicialización con zonas de disponibilidad o subredes diferentes, pero el mismo tipo de instancia y AMI.

Zonas de disponibilidad

La flota de spot inicia las instancias en la subred predeterminada de la zona de disponibilidad de menor precio que ha especificado.

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "KeyName": "my-key-pair",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "m3.medium",
          "Placement": {
              "AvailabilityZone": "us-west-2a, us-west-2b"
          },
          "IamInstanceProfile": {
              "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
          }
      }
  ]
}
```

Subredes

Puede especificar subredes predeterminadas o subredes no predeterminadas, y estas últimas pueden ser de una VPC predeterminada o de una VPC no predeterminada. El servicio de spot inicia las instancias en la subred que está en la zona de disponibilidad de menor precio.

No puede especificar diferentes subredes de la misma zona de disponibilidad en una solicitud de flota de spot.

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "KeyName": "my-key-pair",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
```

```
            }
        ],
        "InstanceType": "m3.medium",
        "SubnetId": "subnet-a61dafcf, subnet-65ea5f08",
        "IamInstanceProfile": {
            "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
        }
    }
  ]
}
```

Si las instancias se inician en una VPC predeterminada, reciben una dirección IPv4 pública de forma predeterminada. Si las instancias se inician en una VPC no predeterminada, no reciben una dirección IPv4 pública de forma predeterminada. Use una interfaz de red en la especificación de inicialización para asignar una dirección IPv4 pública a las instancias iniciadas en una VPC no predeterminada. Si especifica una interfaz de red, debe incluir el ID de subred y el ID de grupo de seguridad mediante la interfaz de red.

```
  ...
    {
        "ImageId": "ami-1a2b3c4d",
        "KeyName": "my-key-pair",
        "InstanceType": "m3.medium",
        "NetworkInterfaces": [
            {
                "DeviceIndex": 0,
                "SubnetId": "subnet-1a2b3c4d",
                "Groups": [ "sg-1a2b3c4d" ],
                "AssociatePublicIpAddress": true
            }
        ],
        "IamInstanceProfile": {
            "Arn": "arn:aws:iam::880185128111:instance-profile/my-iam-role"
        }
    }
  ...
```

Ejemplo 3: inicialización de instancias de spot con el tipo de instancia de menor precio de una lista especificada

En los siguientes ejemplos se describen dos configuraciones de inicialización con tipos de instancias diferentes, pero la misma AMI y zona de disponibilidad o subred. La flota de spot inicia las instancias mediante el tipo de instancia especificado con el menor precio.

Zona de disponibilidad

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "c5.4xlarge",
          "Placement": {
            "AvailabilityZone": "us-west-2b"
          }
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "r3.8xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          }
      }
  ]
}
```

Subred

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "c5.4xlarge",
          "SubnetId": "subnet-1a2b3c4d"
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "r3.8xlarge",
          "SubnetId": "subnet-1a2b3c4d"
      }
  ]
}
```

Ejemplo 4. Anulación del precio para la solicitud

Le recomendamos usar el precio máximo predeterminado, que es el precio bajo demanda. Si lo prefiere, puede especificar un precio máximo para la solicitud de flota y precios máximos para las especificaciones de inicialización individuales.

En los siguientes ejemplos se especifica un precio máximo para la solicitud de flota y precios máximos para dos de las tres especificaciones de inicialización. El precio máximo para la solicitud de flota se usa para cualquier especificación de inicialización que no especifique un precio máximo. La flota de spot inicia las instancias mediante el tipo de instancia con el menor precio.

Zona de disponibilidad

```
{
  "SpotPrice": "1.00",
```

```
  "TargetCapacity": 30,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          },
          "SpotPrice": "0.10"
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.4xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          },
          "SpotPrice": "0.20"
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.8xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          }
      }
    ]
}
```

Subred

```
{
  "SpotPrice": "1.00",
  "TargetCapacity": 30,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.2xlarge",
          "SubnetId": "subnet-1a2b3c4d",
          "SpotPrice": "0.10"
      },
      {
```

```
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c3.4xlarge",
            "SubnetId": "subnet-1a2b3c4d",
            "SpotPrice": "0.20"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c3.8xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        }
    ]
}
```

Ejemplo 5: inicialización de una flota de spot con la estrategia de asignación diversificada

En el siguiente ejemplo se usa la estrategia de asignación `diversified`. Las especificaciones de inicialización tienen tipos de instancias diferentes, pero la misma AMI y zona de disponibilidad o subred. La flota de spot distribuye las 30 instancias entre las tres especificaciones de inicialización, de forma que haya 10 instancias de cada tipo. Para obtener más información, consulte Estrategias de asignación de instancias de spot.

Zona de disponibilidad

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 30,
  "AllocationStrategy": "diversified",
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c4.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          }
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "m3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
```

```
            }
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "r3.2xlarge",
            "Placement": {
                "AvailabilityZone": "us-west-2b"
            }
        }
    ]
}
```

Subred

```
{
    "SpotPrice": "0.70",
    "TargetCapacity": 30,
    "AllocationStrategy": "diversified",
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
    "LaunchSpecifications": [
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c4.2xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "m3.2xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "r3.2xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        }
    ]
}
```

Una práctica recomendada para aumentar la posibilidad de que una solicitud de spot se pueda satisfacer por la capacidad EC2 en caso de interrupción en una de las zonas de disponibilidad consiste en diversificar a través de zonas de disponibilidad. Para esta situación, incluya en la especificación de inicialización todas las zonas de disponibilidad que tenga a su disposición. Y, en

lugar de utilizar la misma subred cada vez, utilice tres subredes únicas (cada una con mapeo a una zona de disponibilidad distinta).

Zona de disponibilidad

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 30,
  "AllocationStrategy": "diversified",
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c4.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2a"
          }
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "m3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          }
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "r3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2c"
          }
      }
  ]
}
```

Subred

```
{
    "SpotPrice": "0.70",
    "TargetCapacity": 30,
    "AllocationStrategy": "diversified",
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
    "LaunchSpecifications": [
```

```
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c4.2xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "m3.2xlarge",
            "SubnetId": "subnet-2a2b3c4d"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "r3.2xlarge",
            "SubnetId": "subnet-3a2b3c4d"
        }
    ]
}
```

Ejemplo 6: inicialización de una flota de spot con ponderación de instancias

En los siguientes ejemplos se usa ponderación de instancias, que significa que el precio se determina por hora de unidad en lugar de por hora de instancia. Cada configuración de inicialización enumera un tipo de instancia y una ponderación diferentes. La flota de spot selecciona el tipo de instancia con el menor precio por hora de unidad. La flota de spot calcula el número de instancias de spot que debe iniciar mediante la división de la capacidad de destino por la ponderación de instancias. Si el resultado no es un entero, la flota de spot lo redondea al siguiente entero, de manera que el tamaño de la flota no esté por debajo de su capacidad de destino.

Si la solicitud de `r3.2xlarge` se realiza con éxito, la spot aprovisiona 4 de estas instancias. Se divide 20 por 6 que da un total de 3,33 instancias, que se redondean a 4 instancias.

Si la solicitud de `c3.xlarge` se realiza con éxito, la spot aprovisiona 7 de estas instancias. Se divide 20 por 3 que da un total de 6,66 instancias, que se redondean a 7 instancias.

Para obtener más información, consulte Ponderación de instancias de flota de spot.

Zona de disponibilidad

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 20,
```

```
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "r3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          },
          "WeightedCapacity": 6
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          },
          "WeightedCapacity": 3
      }
    ]
}
```

Subred

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "r3.2xlarge",
          "SubnetId": "subnet-1a2b3c4d",
          "WeightedCapacity": 6
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.xlarge",
          "SubnetId": "subnet-1a2b3c4d",
          "WeightedCapacity": 3
      }
  ]
}
```

Ejemplo 7: inicialización de una flota de spot con capacidad bajo demanda

Para asegurarse de que dispone siempre de capacidad de instancias, puede incluir una solicitud de capacidad bajo demanda en la solicitud de flota de spot. Si hay capacidad, siempre se cumple la solicitud bajo demanda. El saldo de la capacidad de destino se cumple como spot si hay capacidad y disponibilidad.

En el siguiente ejemplo se especifica una capacidad de destino deseada de 10, de las que 5 unidades deben ser de capacidad bajo demanda. La capacidad de spot no se especifica; sino que está implícita en el saldo de la capacidad de destino menos la capacidad bajo demanda. Amazon EC2 inicia 5 unidades de capacidad como unidades bajo demanda y 5 unidades de capacidad (10 - 5 = 5) como unidades de spot si hay disponibilidad y capacidad de Amazon EC2 disponible.

Para obtener más información, consulte Capacidad bajo demanda en la flota de spot.

```
{
  "IamFleetRole": "arn:aws:iam::781603563322:role/aws-ec2-spot-fleet-tagging-role",
  "AllocationStrategy": "lowestPrice",
  "TargetCapacity": 10,
  "SpotPrice": null,
  "ValidFrom": "2018-04-04T15:58:13Z",
  "ValidUntil": "2019-04-04T15:58:13Z",
  "TerminateInstancesWithExpiration": true,
  "LaunchSpecifications": [],
  "Type": "maintain",
  "OnDemandTargetCapacity": 5,
  "LaunchTemplateConfigs": [
    {
      "LaunchTemplateSpecification": {
        "LaunchTemplateId": "lt-0dbb04d4a6cca5ad1",
        "Version": "2"
      },
      "Overrides": [
        {
          "InstanceType": "t2.medium",
          "WeightedCapacity": 1,
          "SubnetId": "subnet-d0dc51fb"
        }
      ]
    }
  ]
```

```
}
```

Ejemplo 8: configurar el reequilibrio de capacidad para lanzar el reemplazo Instancias de spot

En el siguiente ejemplo, se configura una flota de spot para iniciar una instancia de spot de reemplazo cuando Amazon EC2 emita una recomendación de reequilibrio para una instancia de spot en su flota. Para configurar el reemplazo automático de Instancias de spot para `ReplacementStrategy`, especifique `launch-before-terminate`. Para configurar el retraso de tiempo desde la inicialización de las nuevas instancias de spot de reemplazo hasta la eliminación automática de las instancias de spot anteriores, especifique en `termination-delay` un valor en segundos. Para obtener más información, consulte Opciones de configuración.

> **Note**
>
> Recomendamos utilizar `launch-before-terminate` solo si puede predecir cuánto tiempo tardarán en completarse los procedimientos de cierre de instancias. Esto garantiza que las instancias anteriores terminen solo después de que se hayan completado los procedimientos de cierre. Se cobrará por todas las instancias mientras se ejecutan.

La efectividad de la estrategia de reequilibrio de capacidad depende del número de grupos de capacidades de spot especificados en la solicitud flota de spot. Se recomienda configurar la flota con un conjunto diversificado de tipos de instancia y zonas de disponibilidad y para `AllocationStrategy`especificar `capacityOptimized`. Para obtener más información sobre lo que debe tener en cuenta al momento de configurar una flota de spot para el reequilibrio de la capacidad, consulte Reequilibrio de la capacidad.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "capacityOptimized",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "LaunchTemplate",
                    "Version": "1"
                },
```

```
                "Overrides": [
                      {
                          "InstanceType": "c3.large",
                          "WeightedCapacity": 1,
                          "Placement": {
                              "AvailabilityZone": "us-east-1a"
                          }
                      },
                      {
                          "InstanceType": "c4.large",
                          "WeightedCapacity": 1,
                          "Placement": {
                              "AvailabilityZone": "us-east-1a"
                          }
                      },
                      {
                          "InstanceType": "c5.large",
                          "WeightedCapacity": 1,
                          "Placement": {
                              "AvailabilityZone": "us-east-1a"
                          }
                      }
                ]
          }
    ],
        "TargetCapacity": 5,
        "SpotMaintenanceStrategies": {
            "CapacityRebalance": {
                "ReplacementStrategy": "launch-before-terminate",
                "TerminationDelay": "720"
            }
        }
    }
}
```

Ejemplo 9: lanzamiento de instancias de spot en una flota de capacidad optimizada

En el siguiente ejemplo se demuestra cómo configurar una flota de spot con una estrategia de asignación de spot que optimiza la capacidad. Para optimizar la capacidad, debe establecer `AllocationStrategy` en `capacityOptimized`.

En el siguiente ejemplo, las tres especificaciones de lanzamiento determinan tres grupos de capacidad de spot. La capacidad de destino es de 50 instancias de spot. La flota de spot intenta

iniciar 50 instancias de spot en el grupo de capacidad de spot con capacidad óptima para el número de instancias que va a iniciar.

```
{
    "TargetCapacity": "50",
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "capacityOptimized",
    },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
                 "Overrides": [
                       {
                           "InstanceType": "r4.2xlarge",
                           "AvailabilityZone": "us-west-2a"
                      },
                       {
                           "InstanceType": "m4.2xlarge",
                           "AvailabilityZone": "us-west-2b"
                       },
                       {
                           "InstanceType": "c5.2xlarge",
                           "AvailabilityZone": "us-west-2b"
                       }
                ]
          }
      ]
}
```

Ejemplo 10: lanzamiento de instancias de spot en una flota de capacidad optimizada con prioridades

En el siguiente ejemplo se demuestra cómo configurar una flota de spot con una estrategia de asignación de spot que optimiza la capacidad mientras se utiliza la prioridad sobre la base del mejor esfuerzo.

Cuando se utiliza la estrategia de asignación `capacityOptimizedPrioritized`, puede utilizar el parámetro `Priority` para especificar las prioridades de los grupos de capacidad de spot, donde cuanto menor es el número, mayor es la prioridad. También puede establecer la misma prioridad

para varios grupos de capacidad de spot si los prefiere por igual. Si no establece una prioridad para un grupo, este se considerará último en términos de prioridad.

Para priorizar los grupos de capacidad de spot, debe establecer `AllocationStrategy` en `capacityOptimizedPrioritized`. La flota de spot optimizará primero la capacidad, pero respetará las prioridades sobre la base del mejor esfuerzo (por ejemplo, si el respeto de las prioridades no afecta significativamente la capacidad de la flota de spot para aprovisionar capacidad óptima). Esta es una buena opción para cargas de trabajo en las que se debe minimizar la posibilidad de interrupción y también importa la preferencia por ciertos tipos de instancias.

En el siguiente ejemplo, las tres especificaciones de lanzamiento determinan tres grupos de capacidad de spot. Cada grupo se prioriza, de manera que cuanto menor sea el número, mayor es la prioridad. La capacidad de destino es de 50 instancias de spot. La flota de spot intenta iniciar 50 instancias de spot en el grupo de capacidad de spot con la máxima prioridad sobre la base del mejor esfuerzo, pero optimiza primero la capacidad.

```
{
    "TargetCapacity": "50",
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "capacityOptimizedPrioritized"
    },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
                 "Overrides": [
                        {
                            "InstanceType": "r4.2xlarge",
                            "Priority": 1,
                            "AvailabilityZone": "us-west-2a"
                       },
                        {
                            "InstanceType": "m4.2xlarge",
                            "Priority": 2,
                            "AvailabilityZone": "us-west-2b"
                        },
                        {
                            "InstanceType": "c5.2xlarge",
                            "Priority": 3,
                            "AvailabilityZone": "us-west-2b"
```

```
                    }
                ]
            }
        ]
}
```

Ejemplo 11: inicialización de instancias de spot en una flota priceCapacityOptimized

En el siguiente ejemplo, se muestra cómo configurar una flota de spot con una estrategia de asignación de spot que optimiza tanto para la capacidad como para el precio más bajo. Para optimizar la capacidad, además de tener en cuenta el precio, debe establecer el elemento `AllocationStrategy` de spot en `priceCapacityOptimized`.

En el siguiente ejemplo, las tres especificaciones de lanzamiento determinan tres grupos de capacidad de spot. La capacidad de destino es de 50 instancias de spot. La flota de spot intenta iniciar 50 instancias de spot en el grupo de capacidad de spot con capacidad óptima para la cantidad de instancias que se van a iniciar y, al mismo tiempo, elegir el grupo que tenga el precio más bajo.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "OnDemandAllocationStrategy": "lowestPrice",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::111111111111:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateId": "lt-0123456789example",
                    "Version": "1"
                },
                "Overrides": [
                     {
                          "InstanceType": "r4.2xlarge",
                          "AvailabilityZone": "us-west-2a"
                     },
                     {
                          "InstanceType": "m4.2xlarge",
                          "AvailabilityZone": "us-west-2b"
                     },
                     {
                          "InstanceType": "c5.2xlarge",
```

```
                        "AvailabilityZone": "us-west-2b"
                    }
                ]
            }
        ],
        "TargetCapacity": 50,
        "Type": "request"
    }
}
```

Ejemplo 12: configuración de la selección de tipos de instancia basada en atributos

En el siguiente ejemplo, se muestra cómo configurar una flota de spot para utilizar la selección de tipos de instancia basada en atributos para identificar los tipos de instancia. Para especificar los atributos de instancia necesarios, especifique los atributos en la estructura de `InstanceRequirements`.

En el siguiente ejemplo, se especifican dos atributos de instancia:

- `VCpuCount`: se especifica un mínimo de 2 vCPU. Como no se especifica ningún máximo, no hay ningún límite máximo.
- `MemoryMiB`: se especifica un mínimo de 4 MiB de memoria. Como no se especifica ningún máximo, no hay ningún límite máximo.

Se identificarán los tipos de instancia que tengan 2 o más vCPU y 4 MiB o más de memoria. Sin embargo, la protección de precios y la estrategia de asignación pueden excluir algunos tipos de instancias cuando la flota de spot aprovisiona la flota.

Para obtener una lista y descripciones de todos los atributos posibles que se pueden especificar, consulte InstanceRequirements en la Referencia de la API de Amazon EC2.

```
{
 "AllocationStrategy": "priceCapacityOptimized",
 "TargetCapacity": 20,
 "Type": "request",
 "LaunchTemplateConfigs": [{
  "LaunchTemplateSpecification": {
   "LaunchTemplateName": "my-launch-template",
   "Version": "1"
  },
```

```
  "Overrides": [{
   "InstanceRequirements": {
    "VCpuCount": {
     "Min": 2
    },
    "MemoryMiB": {
     "Min": 4
    }
   }
  }]
 }]
}
```

Cuotas de flota

Las cuotas habituales de Amazon EC2 (anteriormente conocidas como límites) se aplican a las instancias iniciadas por una flota de EC2 o una flota de spot, como los límites de instancias de spot y los límites de volumen.

Además, se aplican las siguientes cuotas:

Descripción de la cuota	Cuota
Cantidad de flotas de EC2 y flotas de spot por región del tipo `maintain` y `request` en los estados `active`, `deleted_running` y `cancelled_running`	1000 [1] [2] [3]
Cantidad de flotas de EC2 del tipo `instant`	Sin límite
Cantidad de grupos de capacidad de spot (combinación única de tipo de instancia y subred) para flotas de EC2 y flotas de spot del tipo `maintain` y `request`	300[1]
Cantidad de grupos de capacidad de spot (combinación única de tipo de instancia y subred) para flotas de EC2 del tipo `instant`	Sin límite

Descripción de la cuota	Cuota
Tamaño de los datos de usuario en una especificación de inicialización	16 KB ²
Capacidad de destino por flota de EC2 o flota de spot	10 000
Capacidad de destino en todas las Flotas de EC2 y Flotas de spot en una región	100 000 ¹
Una solicitud de flota de EC2 o de flota de spot no puede abarcar varias regiones.	
Una solicitud de flota de EC2 o una solicitud de flota de spot no puede abarcar diferentes subredes de la misma zona de disponibilidad.	

¹ Estas cuotas se aplican a sus flotas de EC2 y a sus flotas de spot.

² Se trata de cuotas fijas. No es posible solicitar un aumento de estas cuotas.

³ Después de eliminar una flota de EC2 o cancelar una solicitud de flota de spot, y si se especificó que la flota no debe finalizar sus instancias de spot cuando se eliminó o canceló la solicitud, la solicitud de flota ingresa en el estado `deleted_running` (flota de EC2) o `cancelled_running` (flota de spot) y las instancias siguen ejecutándose hasta que se interrumpan o se terminen manualmente. Si termina las instancias, la solicitud de flota ingresa en el estado `deleted_terminating` (flota de EC2) o `cancelled_terminating` (flota de spot) y no cuenta para calcular esta cuota. Para obtener más información, consulte Eliminar una flota de EC2 y Cancelación de una solicitud de flota de spot.

Solicitar un aumento de la cuota de la capacidad de destino

Si necesita incrementar la cuota predeterminada de la capacidad de destino, puede solicitar un aumento de cuota.

Para solicitar un aumento de la cuota de la capacidad de destino

1. Abra el formulario Crear caso del centro AWS Support.

2. Seleccione Aumento del límite de servicio.
3. En Tipo de límite, elija Flota de EC2.
4. En Región, elija la región de AWS en la que solicita el aumento de la cuota.
5. En Límite, elija Capacidad de flota de destino por flota (en unidades) o Capacidad de flota de destino por región (en unidades), según la cuota que desee aumentar.
6. En Nuevo valor de límite, ingrese el nuevo valor de la cuota.
7. Para solicitar el aumento de otra cuota, elija Agregar otra solicitud y repita los pasos 4 a 6.
8. En Descripción del caso de uso, ingrese el motivo para solicitar un aumento de cuota.
9. En Opciones de contacto, especifique el idioma de contacto y el método de contacto preferidos.
10. Seleccione Submit (Enviar).

Monitorear Amazon EC2

El monitoreo es un aspecto importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) y las soluciones de AWS. Es conveniente recopilar datos de monitoreo de todas las partes de las soluciones de AWS para que sea más sencillo depurar un error que se produce en distintas partes del código, en caso de que ocurra. No obstante, antes de comenzar a monitorear Amazon EC2, debería crear un plan de monitorización que incluyera lo siguiente:

- ¿Cuáles son los objetivos del monitoreo?
- ¿Qué recursos va a monitorizar?
- ¿Con qué frecuencia va a supervisar estos recursos?
- ¿Qué herramientas de monitoreo va a utilizar?
- ¿Quién se encargará de realizar las tareas de monitoreo?
- ¿Quién debería recibir una notificación cuando surjan problemas?

Después de definir los objetivos y de crear el plan de monitoreo, el paso siguiente consiste en establecer un punto de referencia para el desempeño normal de Amazon EC2 en el entorno. Conviene medir el desempeño de Amazon EC2 en varias ocasiones y con diferentes condiciones de carga. A medida que monitorea Amazon EC2, guarde un historial de los datos de monitoreo que recopila. Puede comparar el desempeño actual de Amazon EC2 con los datos históricos para identificar patrones de desempeño normal y anomalías en el desempeño, así como desarrollar métodos para solucionarlos. Por ejemplo, puede monitorizar el uso de la CPU, la I/O de disco y el uso de la red de las instancias de EC2. Si el desempeño no alcanza los valores del punto de referencia establecido, es posible que deba volver a configurar u optimizar la instancia para reducir la utilización de la CPU, mejorar la E/S de disco o reducir el tráfico de red.

Para establecer un punto de referencia debe, como mínimo, monitorizar los elementos siguientes:

Elementos que se van a monitorear	Métrica de Amazon EC2	Monitoreo del agente/CloudWatch Logs
Utilización de la CPU	CPUUtilization	
Utilización de la red	NetworkIn	

Elementos que se van a monitorear	Métrica de Amazon EC2	Monitoreo del agente/CloudWatch Logs
	NetworkOut	
Desempeño de disco	DiskReadOps DiskWriteOps	
Escrituras/lecturas en disco	DiskReadBytes DiskWriteBytes	
Utilización de memoria, utilización de intercambio de disco, utilización de espacio de disco, utilización de archivo de página, recopilación de registros		[Instancias de Linux y Windows Server] Recopilar métricas y registros de instancias de Amazon EC2 y servidores locales con el Agente de CloudWatch [Migración desde el agente de CloudWatch Logs anterior en instancias de Windows Server] Migrar la colección de registros de instancia de Windows Server al agente de CloudWatch

Monitoreo automatizado y manual

AWS proporciona varias herramientas que puede usar para monitorear Amazon EC2. Puede configurar algunas de estas herramientas para que monitoreen por usted, pero otras herramientas requieren intervención manual.

Herramientas de monitoreo

- Herramientas de monitoreo automatizadas
- Herramientas de monitoreo manuales

Herramientas de monitoreo automatizadas

Puede utilizar las siguientes herramientas de monitoreo automatizada para vigilar Amazon EC2 y recibir información cuando algo va mal:

- Comprobaciones de estado de sistemas: monitorea los sistemas de AWS necesarios para usar la instancia y garantiza que funcionan correctamente. Estas comprobaciones detectan problemas con la instancia que requieren la intervención de AWS para su reparación. Cuando una comprobación de estado del sistema da error, puede elegir entre esperar a que AWS corrija el problema o solucionarlo manualmente (por ejemplo: al parar y reiniciar la instancia, o bien, al terminar y reemplazar una instancia). Entre los ejemplos de problemas que provocan errores en las comprobaciones de estado del sistema se incluyen:
  - Pérdida de conectividad de red
  - Pérdida de potencia del sistema
  - Problemas de software en el host físico
  - Problemas de hardware en el host físico que afectan a la accesibilidad a la red

  Para obtener más información, consulte Comprobaciones de estado para sus instancias.
- Comprobaciones de estado de instancias: monitoree la configuración de software y de red de la instancia individual. Estas comprobaciones detectan problemas que requieren su implicación para la reparación. Cuando una comprobación de estado de instancias da error, por lo general, deberá resolver el problema manualmente (por ejemplo, reiniciando la instancia o efectuando modificaciones en el sistema operativo). Entre los ejemplos de problemas que pueden provocar errores en las comprobaciones de estado de la instancia se incluyen:
  - Error de las comprobaciones de estado del sistema
  - Configuración de red o de inicio incorrecta
  - Memoria agotada
  - Sistema de archivos dañado
  - Kernel incompatible

  Para obtener más información, consulte Comprobaciones de estado para sus instancias.
- Alarmas de Amazon CloudWatch: vigile una única métrica durante el período especificado y realice una o varias acciones según el valor de la métrica relativo a un determinado umbral durante varios períodos de tiempo. La acción es una notificación que se envía a un tema de Amazon Simple Notification Service (Amazon SNS) o a una política de Amazon EC2 Auto Scaling. Las

alarmas invocan acciones únicamente para los cambios de estado prolongados. Las alarmas de CloudWatch no invocarán acciones tan solo por tener un estado determinado; es necesario que el estado haya cambiado y se mantenga durante un número específico de periodos. Para obtener más información, consulte Monitorear las instancias con CloudWatch.

- Amazon EventBridge: automatice los servicios de AWS y responda automáticamente a los eventos del sistema. Los eventos de los servicios de AWS llegan a EventBridge prácticamente en tiempo real y puede especificar acciones automatizadas para cuando un evento coincide con una de las reglas que ha escrito. Para obtener más información, consulte ¿Qué es Amazon EventBridge?.
- Amazon CloudWatch Logs: monitoree, almacene y tenga acceso a los archivos de registro desde instancias de Amazon EC2, AWS CloudTrail u otras fuentes. Para obtener más información, consulte la Guía del usuario de Amazon CloudWatch Logs.
- Agente de CloudWatch: recopila registros y métricas de nivel de sistema tanto desde hosts como invitados en las instancias de EC2 y servidores en las instalaciones. Para obtener más información, consulte Recopilación de métricas y registros de instancias Amazon EC2 y servidores locales con el agente de CloudWatch en la Guía del usuario de Amazon CloudWatch.

Herramientas de monitoreo manuales

Otra parte importante del monitoreo de Amazon EC2 implica el monitoreo manual de los elementos que no cubren los scripts, las comprobaciones de estado y las alarmas de CloudWatch. Los paneles de consola de Amazon EC2 y de CloudWatch proporcionan una vista rápida del entorno de Amazon EC2.

- El panel de Amazon EC2 muestra:
  - El estado del servicio y los eventos programados por región
  - El estado de la instancia
  - Las comprobaciones de estado
  - El estado de la alarma
  - Detalles de las métricas de la instancia (en el panel de navegación, elija Instances [Instancias], seleccione una instancia y elija la pestaña Monitoring [Monitoreo])
  - Detalles de las métricas del volumen (en el panel de navegación, elija Volumes [Volúmenes], seleccione un volumen y elija la pestaña Monitoring [Monitoreo])
- El panel de Amazon CloudWatch muestra:
  - Alarmas y estado actual

- Gráficos de alarmas y recursos
- Estado de los servicios

Además, puede utilizar CloudWatch para hacer lo siguiente:

- Gráfico con los datos de monitoreo de Amazon EC2 para solucionar problemas y descubrir tendencias
- Buscar y examinar todas sus métricas de recursos de AWS.
- Crear y editar las alarmas de notificación de problemas
- Consultar información general sobre alarmas y recursos de AWS

Prácticas recomendadas de monitoreo

Aplique las siguientes prácticas recomendadas de monitoreo como ayuda con las tareas de monitorización de Amazon EC2.

- Haga del monitoreo una prioridad para solventar pequeñas cuestiones antes de que se conviertan en grandes problemas.
- Cree e implemente un plan de monitoreo para recopilar datos de todos los componentes de la solución de AWS, de forma que resulte más sencillo depurar un error que se produce en distintas partes del código, en caso de que ocurra. El plan de monitoreo debería responder, como mínimo, a las preguntas siguientes:
  - ¿Cuáles son los objetivos del monitoreo?
  - ¿Qué recursos va a monitorizar?
  - ¿Con qué frecuencia va a supervisar estos recursos?
  - ¿Qué herramientas de monitoreo va a utilizar?
  - ¿Quién se encargará de realizar las tareas de monitoreo?
  - ¿Quién debería recibir una notificación cuando surjan problemas?
- Automatice las tareas de monitoreo en la medida de lo posible.
- Compruebe los archivos de registro de las instancias de EC2.

Monitorear el estado de las instancias

Se puede monitorizar el estado de las instancias mediante la visualización de comprobaciones de estado y eventos programados para las instancias.

Una comprobación de estado le ofrece la información que resulta de las comprobaciones automatizadas realizadas por Amazon EC2. Estas comprobaciones automatizadas detectan si hay problemas específicos que afecten a sus instancias. La información de comprobación de estado, junto con los datos proporcionados por Amazon CloudWatch, le ofrecen visibilidad operativa detallada de cada una de las instancias.

También puede ver el estado de eventos específicos que están programados para las instancias. El estado de os eventos proporcionan información acerca de las próximas actividades planificadas para sus instancias, como rearranque o retirada. También proporcionan la hora de inicio y fin planificadas de cada evento.

Contenido

Comprobaciones de estado para sus instancias

Con el monitoreo de estado de las instancias, puede determinar rápidamente si Amazon EC2 ha detectado algún problema que pudiera impedir a las instancias ejecutar aplicaciones. Amazon EC2 realiza verificaciones automatizadas en cada instancia de EC2 en ejecución para identificar problemas de hardware y de software. Puede ver los resultados de estas comprobaciones de estado para identificar problemas específicos y detectables. Estos datos de estado de eventos aumentan la información que Amazon EC2 ya proporciona acerca del estado previsto de cada instancia (como `pending`, `running` y `stopping`) y las métricas de utilización que Amazon CloudWatch monitoriza (uso de la CPU, tráfico de red y actividad de disco).

Las comprobaciones de estado se realizan cada minuto y devuelven un estado de aprobación o error. Si se superan todas las comprobaciones, el estado general de la instancia es OK (CORRECTO). Si no se supera una o varias comprobaciones, el estado general es impaired (deteriorado). Las comprobaciones de estado están integradas en Amazon EC2, de manera que no se pueden deshabilitar ni eliminar.

Cuando no se supera una comprobación de estado, la métrica de CloudWatch correspondiente a las comprobaciones de estado aumenta. Para obtener más información, consulte Métricas de comprobación de estado. Puede utilizar estas métricas para crear alarmas de CloudWatch que se activen en función del resultado de las comprobaciones de estado. Por ejemplo, puede crear una alarma que le advierta si las comprobaciones de estado fallan en una instancia específica. Para obtener más información, consulte Crear y editar alarmas de comprobación de estado.

También puede crear una alarma de Amazon CloudWatch que monitorice una instancia Amazon EC2 y recupere automáticamente la instancia si su estado se deteriora debido a un problema subyacente. Para obtener más información, consulte Resiliencia de las instancias.

Contenido

Tipos de comprobaciones de estado

Hay tres tipos de comprobaciones de estado.

Comprobaciones de estado de sistemas

Las comprobaciones de estado del sistema monitorean los sistemas de AWS en los que se ejecuta la instancia. Estas comprobaciones detectan problemas subyacentes con la instancia que requieren la intervención de AWS para su reparación. Cuando una comprobación de estado de sistemas falla, puede elegir esperar a que AWS repare el problema o puede resolverlo por su cuenta. En el caso de las instancias respaldadas por Amazon EBS, puede detener e iniciar la instancia usted mismo, lo que en la mayoría de los escenarios hace que la instancia migre a un nuevo host. Para instancias de Linux respaldadas por un almacén de instancias, puede terminar y reemplazar la instancia. Para las instancias de Windows, el volumen raíz debe ser un volumen de Amazon EBS; no se admite el almacén de instancias para el volumen raíz. Tenga en cuenta que los volúmenes del almacén de instancias son efímeros y que todos los datos se pierden cuando se detiene la instancia.

A continuación se muestran ejemplos de problemas que pueden provocar errores en las comprobaciones de estado del sistema:

- Pérdida de conectividad de red
- Pérdida de potencia del sistema
- Problemas de software en el host físico
- Problemas de hardware en el host físico que afectan a la accesibilidad a la red

Si se produce un error en la comprobación del estado de un sistema, aumentamos la métrica StatusCheckFailed_System.

instancias Bare Metal

Si realiza un reinicio desde el sistema operativo en una instancia de Bare Metal, la comprobación del estado del sistema podría devolver temporalmente un estado de error. Cuando la instancia esté disponible, la comprobación de estado del sistema debería devolver un estado de aprobado.

Comprobaciones de estado de instancias

Comprobaciones de estado de instancias: monitoree la configuración de software y de red de la instancia individual. Amazon EC2 verifica el estado de la instancia mediante el envío de una solicitud del protocolo de resolución de direcciones (ARP) a la interfaz de red (NIC). Estas comprobaciones detectan problemas que requieren su implicación para la reparación. Cuando una comprobación de estado de instancias falla, debe resolver el problema por sí mismo (por ejemplo, reiniciando la instancia o realizando cambios en la configuración de la instancia).

> **Note**
>
> Las distribuciones de Linux recientes que utilizan `systemd-networkd` para la configuración de red pueden informar sobre las comprobaciones de estado de forma diferente a las distribuciones anteriores. Durante el proceso de arranque, este tipo de red puede iniciarse antes y, posiblemente, terminar antes que otras tareas de inicio, lo que también puede afectar al estado de la instancia. Las comprobaciones de estado que dependen de la disponibilidad de la red pueden informar un estado correcto antes de que se completen otras tareas.

A continuación se muestran ejemplos de problemas que pueden provocar errores en las comprobaciones de estado de la instancia:

- Error de las comprobaciones de estado del sistema
- Configuración de red o de inicio incorrecta
- Memoria agotada
- Sistema de archivos dañado
- Kernel incompatible
- [Instancias de Windows] Durante el reinicio de una instancia o al empaquetar una instancia con respaldo en el almacén de instancias de Windows, una comprobación de estado de la instancia informa de un fallo hasta que la instancia vuelve a estar disponible.

Si se produce un error en la comprobación del estado de una instancia, incrementamos la métrica StatusCheckFailed_Instance.

instancias Bare Metal

Si realiza un reinicio desde el sistema operativo en una instancia de Bare Metal, la comprobación del estado de la instancia podría devolver temporalmente un estado de error. Cuando la instancia esté disponible, la comprobación de estado de la instancia debería devolver un estado de aprobado.

Comprobaciones de estado de EBS adjuntas

Las comprobaciones de estado de EBS adjuntas supervisan si se puede acceder a los volúmenes de Amazon EBS adjuntos a una instancia y completar operaciones de E/S. La métrica `StatusCheckFailed_AttachedEBS` es un valor binario que indica que hay problemas si uno o varios de los volúmenes de EBS adjuntos a la instancia no pueden completar las operaciones de E/S. Estas comprobaciones de estado detectan problemas subyacentes en la computación o la infraestructura de Amazon EBS. Si la métrica de comprobación de estado de EBS adjunta falla, puede esperar a que AWS resuelva el problema o tomar medidas, como reemplazar los volúmenes afectados o detener y reiniciar la instancia.

A continuación se muestran ejemplos de problemas que pueden provocar errores en las comprobaciones de estado de EBS adjuntas:

- Problemas de hardware o software en los subsistemas de almacenamiento subyacentes a los volúmenes de EBS
- Problemas de hardware en el host físico que afectan a la accesibilidad de los volúmenes de EBS

- Problemas de conectividad entre la instancia y los volúmenes de EBS

Puede usar la métrica `StatusCheckFailed_AttachedEBS` para ayudar a mejorar la resiliencia de su carga de trabajo. Puede utilizar esta métrica para crear alarmas de Amazon CloudWatch que se activen en función del resultado de la comprobación de estado. Por ejemplo, puede realizar una conmutación por error en una instancia secundaria o una zona de disponibilidad si detecta un impacto prolongado. Como alternativa, puede supervisar el rendimiento de E/S de cada volumen adjunto mediante las métricas de EBS de CloudWatch para detectar y reemplazar el volumen dañado. Si su carga de trabajo no impulsa la E/S a ninguno de los volúmenes de EBS adjuntos a su instancia y la comprobación de estado de EBS adjunta indica que hay un problema, puede detener e iniciar la instancia para solucionar los problemas con el host físico que están afectando a la accesibilidad de los volúmenes de EBS. Para obtener más información, consulte Métricas de Amazon CloudWatch para Amazon EBS.

> **Note**
>
> - La métrica de comprobación de estado de EBS adjunta solo está disponible para las instancias Nitro.
> - Puede supervisar la métrica de comprobación de estado de EBS adjunta al crear una alarma de CloudWatch basada en la métrica `StatusCheckFailed_AttachedEBS`. No puede ver esta comprobación de estado con el comando de la AWS CLI describe-instance-status.

Uso de comprobaciones de estado

Puede usar comprobaciones de estado mediante la consola y las herramientas de línea de comandos, como la AWS CLI.

Temas

- Ver comprobaciones de estado
- Crear y editar alarmas de comprobación de estado

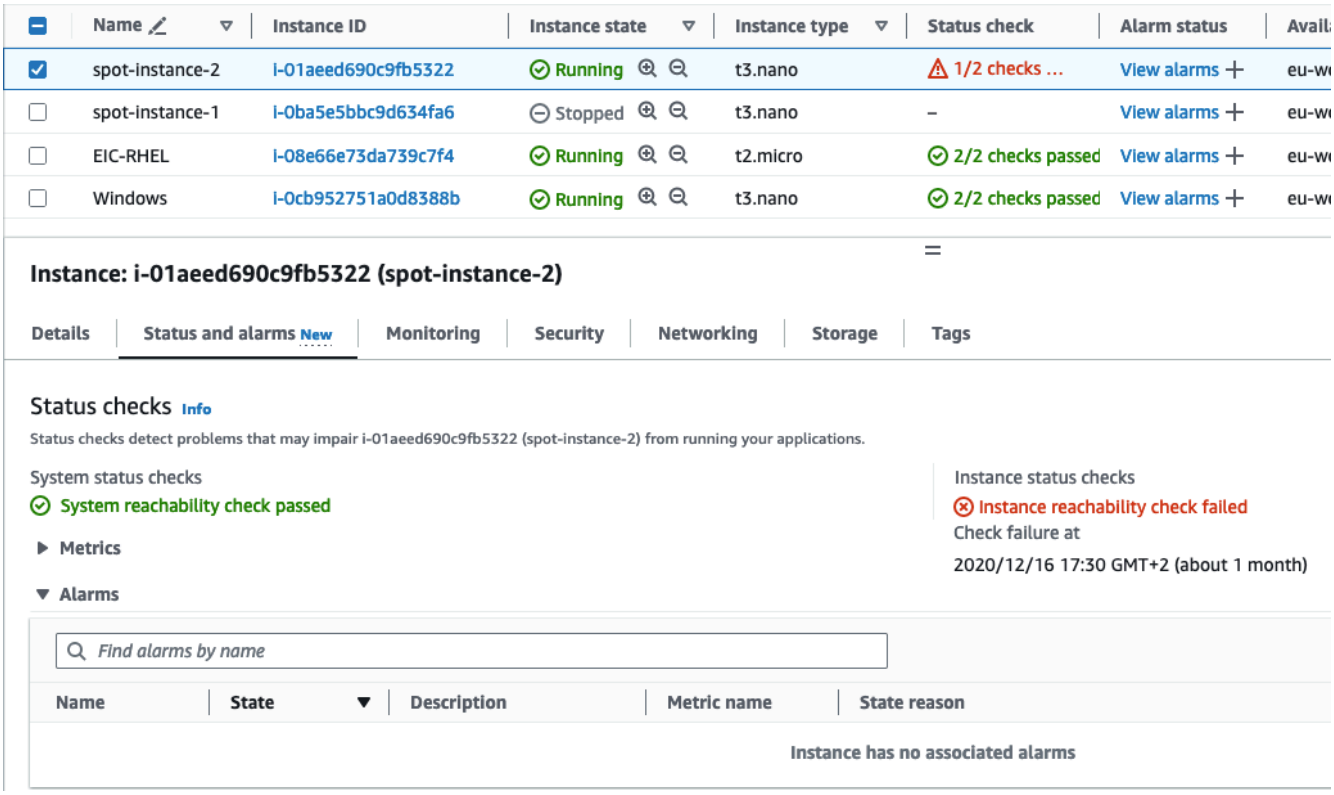
Ver comprobaciones de estado

Para ver las comprobaciones de estado, use uno de los siguientes métodos:

Console

Para ver comprobaciones de estado

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancias).
3. En la página Instances (Instancias), en la columna Status Checks (Comprobaciones de estado), se indica el estado operativo de cada instancia.
4. Para ver el estado de una instancia específica, seleccione la instancia y, a continuación, elija la pestaña Estado y alarmas.



Si la instancia tiene una comprobación de estado fallida, normalmente debe solucionar el problema por su cuenta (por ejemplo: al reiniciar la instancia o realizar cambios en la configuración de la instancia). Para solucionar los errores de comprobación de estado del sistema o la instancia en instancias de Linux, consulte Solución de problemas de las instancias de Linux con comprobaciones de estado no superadas.

5. Para revisar las métricas de CloudWatch sobre las comprobaciones de estado, en la pestaña Estado y alarmas, amplíe Métricas para ver los gráficos de las siguientes métricas:

   - Comprobación de estado no superada para el sistema

- Comprobación de estado no superada para la instancia

Para obtener más información, consulte the section called “Métricas de comprobación de estado”.

Command line

Para ver las comprobaciones de estado de las instancias de ejecución, puede utilizar el comando describe-instance-status (AWS CLI).

Para ver el estado de todas las instancias, utilice el siguiente comando.

```
aws ec2 describe-instance-status
```

Para obtener el estado de todas las instancias con un estado `impaired`, use el siguiente comando.

```
aws ec2 describe-instance-status \
    --filters Name=instance-status.status,Values=impaired
```

Para obtener el estado de una única instancia, use el siguiente comando.

```
aws ec2 describe-instance-status \
    --instance-ids i-1234567890abcdef0
```

También puede usar los siguientes comandos:

- Get-EC2InstanceStatus (AWS Tools for Windows PowerShell)
- DescribeInstanceStatus (API de consultas de Amazon EC2)

Si tiene una instancia de Linux con una comprobación de estado no superada, consulte Solución de problemas de las instancias de Linux con comprobaciones de estado no superadas.

Crear y editar alarmas de comprobación de estado

Puede utilizar las métricas de comprobación de estado para crear alarmas de CloudWatch que le avisen cuando una instancia no haya superado la comprobación de estado.

> **Important**
>
> Las comprobaciones de estado y las alarmas de comprobación de estado pueden mostrar temporalmente un estado de datos insuficientes si faltan puntos de datos de las métricas. Aunque es poco frecuente, esto puede ocurrir cuando se produce una interrupción en los sistemas de generación de informes de las métricas, incluso cuando una instancia está en buen estado. Le recomendamos que entienda este estado como un aviso de que faltan datos y no como un error en la comprobación del estado ni una interrupción de la alarma, en especial cuando se toman acciones de detención, finalización, reinicio o recuperación de la instancia como respuesta.

Para crear una alarma de comprobación de estado, use uno de los siguientes métodos:

Console

Utilice el procedimiento siguiente para configurar una alarma que le envíe una notificación por correo electrónico o detenga, termine o recupere una instancia cuando no haya superado una comprobación de estado.

Para crear una alarma de comprobación de estado

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancias).
3. Seleccione la instancia, elija la pestaña Status Checks (Comprobaciones de estado), seleccione Actions (Acciones) y haga clic en Create status check alarm (Crear alarma de comprobación de estado).
4. En la página Manage CloudWatch alarms (Administrar alarmas de CloudWatch), en Add or edit alarm (Agregar o editar alarma), elija Create an alarm (Crear una alarma).
5. En Alarm notification (Notificación de alarma), active la opción para configurar las notificaciones de Amazon Simple Notification Service (Amazon SNS). Seleccione un tema de Amazon SNS existente o escriba un nombre para crear un nuevo tema.

   Si agrega una dirección de correo electrónico a la lista de destinatarios o crea un tema nuevo, Amazon SNS envía un correo electrónico de confirmación de suscripción a cada dirección nueva. Cada destinatario debe confirmar la suscripción seleccionando el enlace incluido en ese mensaje. Las notificaciones de alertas solo se envían a direcciones confirmadas.

6. En Alarm action (Acción de la alarma), active la opción para especificar la acción que debe llevarse a cabo cuando se active la alarma. Seleccione la acción.
7. En Alarm thresholds (Umbrales de alarma), especifique la métrica y los criterios para la alarma.

   Puede dejar la configuración predeterminada de Group samples by (Average) (Agrupar muestras por [Promedio]) y Type of data to sample (Status check failed:either) (Tipo de datos para muestra [Comprobación de estado no superada: cualquiera]), o bien cambiarla para que se adapte a sus necesidades.

   En Consecutive Period (Periodo consecutivo), establezca el número de periodos a evaluar y, en Period (Periodo), especifique la duración del periodo de evaluación antes de que se active la alarma y se envíe un correo electrónico.
8. (Opcional) En Sample metric data (Muestrear datos de métrica), elija Add to dashboard (Agregar al panel).
9. Seleccione Create (Crear).

Si necesita realizar cambios a una alarma de estado de instancia, puede editarla.

Para editar una alarma de comprobación de estado

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancias).
3. Seleccione la instancia y elija Actions (Acciones), Monitoring (Monitoreo), Manage CloudWatch alarms (Administrar alarmas de CloudWatch).
4. En la página Manage CloudWatch alarms (Administrar alarmas de CloudWatch), en Add or edit alarm (Agregar o editar alarma), elija Edit an alarm (Editar una alarma).
5. En Search for alarm (Buscar alarma), elija la alarma.
6. Cuando termine de realizar los cambios, elija Update (Actualizar).

Command line

En el siguiente ejemplo, la alarma publica una notificación a un tema de SNS, `arn:aws:sns:us-west-2:111122223333:my-sns-topic`, cuando la instancia no supera la comprobación de instancia o la comprobación de estado de sistema durante al menos dos periodos consecutivos. La metríca de CloudWatch utilizada es `StatusCheckFailed`.

Para crear una alarma de comprobación de estado mediante la AWS CLI

1. Seleccione un tema de SNS existente o cree uno nuevo. Para obtener más información, consulte Utilización de AWS CLI con Amazon SNS en la Guía del usuario de AWS Command Line Interface.
2. Utilice el siguiente comando list-metrics para ver las métricas de Amazon CloudWatch disponibles para Amazon EC2:

```
aws cloudwatch list-metrics --namespace AWS/EC2
```

3. Use el siguiente comando put-metric-alarm para crear la alarma:

```
aws cloudwatch put-metric-alarm \
    --alarm-name StatusCheckFailed-Alarm-for-i-1234567890abcdef0 \
    --metric-name StatusCheckFailed \
    --namespace AWS/EC2 \
    --statistic Maximum \
    --dimensions Name=InstanceId,Value=i-1234567890abcdef0 \
    --unit Count \
    --period 300 \
    --evaluation-periods 2 \
    --threshold 1 \
    --comparison-operator GreaterThanOrEqualToThreshold \
    --alarm-actions arn:aws:sns:us-west-2:111122223333:my-sns-topic
```

El periodo del intervalo de tiempo, en segundo, durante el que se recopilan métricas de Amazon CloudWatch. Este ejemplo utiliza 300, que es igual a 60 segundos multiplicados por 5 minutos. El periodo de evaluación es el número de periodos consecutivos durante los que se debe comparar el valor de la métrica con el umbral. En este ejemplo se utiliza 2. Las acciones de alarma son las acciones que se realizan cuando se activa esta alarma. Este ejemplo configura la alarma para enviar un correo electrónico mediante Amazon SNS.

Eventos de cambio de estado de sus instancias

Amazon EC2 envía un evento `EC2 Instance State-change Notification` a Amazon EventBridge cuando una instancia cambia de estado.

El siguiente es un ejemplo de los datos de este evento. En este ejemplo, la instancia ingresó al estado `pending`.

```
{
   "id":"7bf73129-1428-4cd3-a780-95db273d1602",
   "detail-type":"EC2 Instance State-change Notification",
   "source":"aws.ec2",
   "account":"123456789012",
   "time":"2021-11-11T21:29:54Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:ec2:us-east-1:123456789012:instance/i-abcd1111"
   ],
   "detail":{
      "instance-id":"i-abcd1111",
      "state":"pending"
   }
}
```

Los valores posibles de `state` son:

- `pending`
- `running`
- `stopping`
- `stopped`
- `shutting-down`
- `terminated`

Cuando se lanza o inicia una instancia, esta ingresa al estado `pending` y, a continuación, al estado `running`. Cuando se detiene una instancia, esta ingresa al estado `stopping` y, a continuación, al estado `stopped`. Cuando se termina una instancia, esta ingresa al estado `shutting-down` y, a continuación, al estado `terminated`.

Reciba una notificación por correo electrónico cuando una instancia cambie de estado

Para recibir notificaciones por correo electrónico cuando su instancia cambie de estado, cree un tema de Amazon SNS y, luego, cree una regla de EventBridge para el evento `EC2 Instance State-change Notification`.

Para crear un tema de SNS

1. Abra la consola de Amazon SNS en https://console.aws.amazon.com/sns/v3/home.

2. En el panel de navegación, elija Temas.
3. Elija Crear nuevo tema.
4. En Tipo, seleccione Estándar.
5. En Nombre, ingrese un nombre para el tema.
6. Elija Crear nuevo tema.
7. Elija Crear una suscripción.
8. En Protocolo, elija Correo electrónico.
9. En Punto de conexión, ingrese una dirección de correo electrónico para recibir las notificaciones.
10. Seleccione Crear una suscripción.
11. Recibirá un mensaje de correo electrónico con la siguiente línea de asunto: AWS Notification - Subscription Confirmation. Siga las instrucciones para confirmar la suscripción.

Para crear una regla de EventBridge

1. Abra la consola de Amazon EventBridge en https://console.aws.amazon.com/events/.
2. Elija Crear regla.
3. En Nombre, ingrese un nombre para la regla.
4. En Tipo de regla, elija Regla con un patrón de evento.
5. Elija Siguiente.
6. En Event pattern (Patrón de eventos), realice una de las siguientes acciones:
    a. En Origen del evento, elija Servicios de AWS.
    b. En Servicio de AWS, elija EC2.
    c. En Event Type (Tipo de evento), elija EC2 Instance State-change Notification (Notificación de cambio de estado de instancia de EC2).
    d. De forma predeterminada, enviamos notificaciones sobre cualquier cambio de estado de cualquier instancia. Si lo prefiere, puede seleccionar estados o instancias específicos.
7. Elija Siguiente.
8. Especifique un destino de la siguiente manera:
    a. Para Target types (Tipos de destino), elija Servicio de AWS.
    b. Para Select a target (Seleccione un destino), elija SNS topic (Tema de SNS).

c. En Topic (Tema), elija el tema de SNS que creó en el procedimiento anterior.

9. Elija Siguiente.
10. (Opcional) Añada etiquetas a la regla.
11. Elija Siguiente.
12. Seleccione Crear regla.
13. Para probar la regla, inicie un cambio de estado. Por ejemplo, iniciar una instancia detenida, detener una instancia en ejecución o lanzar una instancia. Recibirá mensajes de correo electrónico con la siguiente línea de asunto: AWS Notification Message. El cuerpo del correo electrónico contendrá los datos del evento.

Eventos programados para las instancias

AWS puede programar eventos para las instancias, como un reinicio, una detención o un inicio, o una retirada. Estos eventos no ocurren con frecuencia. Si una de las instancias se verá afectada por un evento programado, AWS envía un email a la dirección asociada con su cuenta de AWS antes del evento programado. El correo electrónico proporciona información acerca del evento, incluida la fecha de inicio y de finalización. En función del evento, es posible que pueda tomar medidas para controlar el tiempo del evento. AWS también envía un evento de AWS Health, que puede monitorear y administrar con Amazon CloudWatch Events. Para obtener más información acerca del monitoreo de eventos de AWS Health con CloudWatch, consulte Monitoreo de eventos de AWS Health con CloudWatch Events.

AWS administra los eventos programados; no puede programar eventos para sus instancias. Puede ver los eventos programados por AWS, personalizar las notificaciones de eventos programados para incluir o eliminar etiquetas de la notificación por email y llevar a cabo diferentes acciones cuando una instancia está programada para su reinicio, retirada o detención.

Para actualizar la información de contacto de la cuenta con el fin de asegurarse de que recibe las notificaciones sobre los eventos programados, vaya a la página Configuración de la cuenta.

> **Note**
>
> Cuando una instancia se ve afectada por un evento programado y forma parte de un grupo de escalado automático, Amazon EC2 Auto Scaling la sustituye eventualmente como parte de sus comprobaciones de estado, sin que sea necesario realizar más acciones por su parte. Para obtener más información acerca de las comprobaciones de estado realizadas

por Amazon EC2 Auto Scaling, consulte Comprobaciones de estado para instancias de Auto Scaling en la Guía del usuario de Amazon EC2 Auto Scaling.

Contenido

Tipos de eventos programados

Amazon EC2 puede crear los siguientes tipos de eventos para las instancias, donde el evento se produce a una hora programada:

- Instance stop (Detención de instancia): a la hora programada, la instancia se detiene. Cuando vuelva a iniciarla, la instancia migrará a un nuevo host. Solo se aplica a instancias respaldadas por Amazon EBS.
- Instance retirement (Retirada de la instancia): a la hora programada, la instancia se detiene si está respaldada por Amazon EBS o se terminará si está respaldada por un almacén de instancias.
- Instance reboot (rearranque de instancia): a la hora programada, la instancia se vuelve a arrancar.
- System reboot (rearranque de sistema): a la hora programada, el host de la instancia se vuelve a arrancar.
- System maintenance (Mantenimiento del sistema): a la hora programada, la instancia podría verse temporalmente afectada por un mantenimiento de red o de energía.

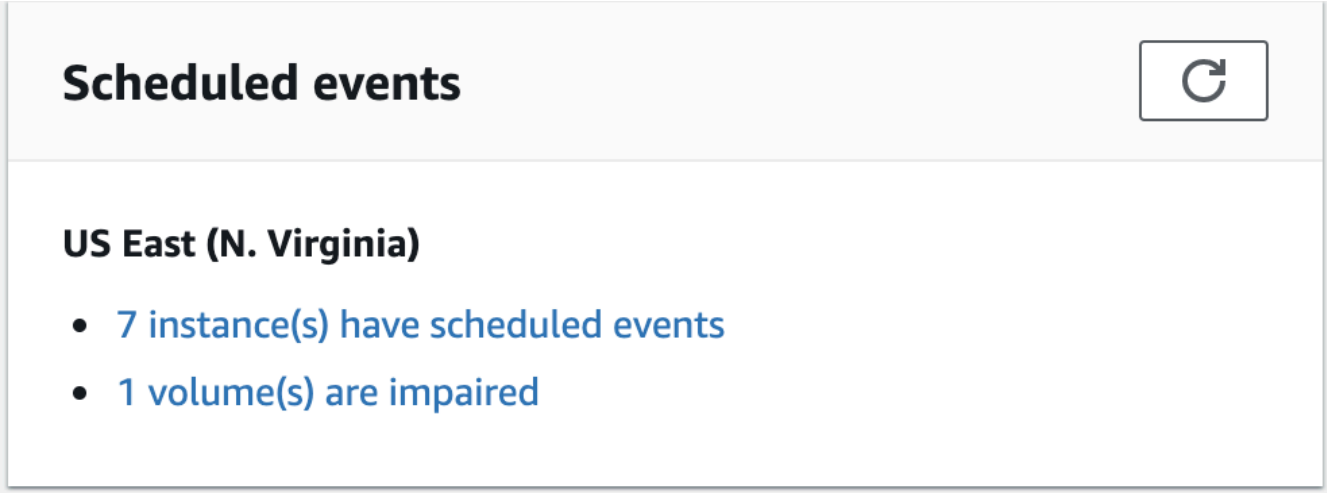
Ver eventos programados

Además de recibir notificaciones de eventos programados por email, puede consultar los eventos programados mediante uno de los siguientes métodos.

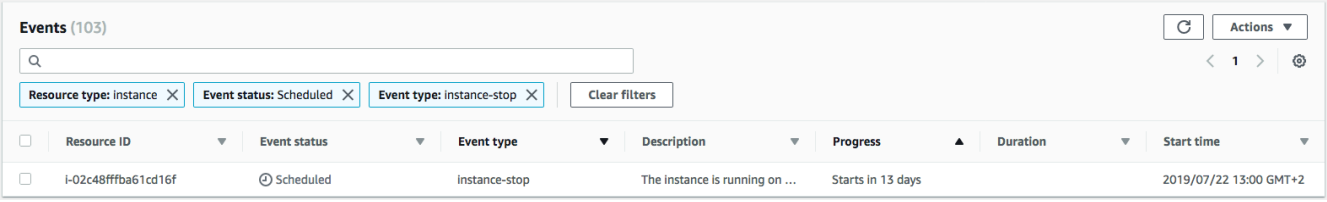
Console

Para ver eventos programados para las instancias

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. El panel muestra todos los recursos con un evento asociado en Eventos programados.



3. En el panel de navegación, elija Eventos para obtener más información. Se muestran todos los recursos con un evento asociado. Puede filtrar por características como el tipo de evento, el tipo de recurso y la zona de disponibilidad.



AWS CLI

Para ver eventos programados para las instancias

Utilice el comando describe-instance-status.

```
aws ec2 describe-instance-status \
    --instance-id i-1234567890abcdef0 \
    --query "InstanceStatuses[].Events"
```

La siguiente salida de ejemplo muestra un evento de reinicio.

```
[
```

```
    "Events": [
        {
            "InstanceEventId": "instance-event-0d59937288b749b32",
            "Code": "system-reboot",
            "Description": "The instance is scheduled for a reboot",
            "NotAfter": "2019-03-15T22:00:00.000Z",
            "NotBefore": "2019-03-14T20:00:00.000Z",
            "NotBeforeDeadline": "2019-04-05T11:00:00.000Z"
         }

    ]
]
```

A continuación se muestra un ejemplo del resultado que muestra un evento de retirada de la instancia.

```
[
    "Events": [
        {
            "InstanceEventId": "instance-event-0e439355b779n26",

            "Code": "instance-stop",
            "Description": "The instance is running on degraded hardware",
            "NotBefore": "2015-05-23T00:00:00.000Z"
        }
    ]
]
```

PowerShell

Para ver eventos programados para las instancias mediante la AWS Tools for Windows PowerShell

Utilice el siguiente comando Get-EC2InstanceStatus.

```
PS C:\> (Get-EC2InstanceStatus -InstanceId i-1234567890abcdef0).Events
```

A continuación se muestra un ejemplo del resultado que muestra un evento de retirada de la instancia.

```
Code         : instance-stop
Description  : The instance is running on degraded hardware
```

```
NotBefore    : 5/23/2015 12:00:00 AM
```

Instance metadata

Para ver eventos programados para las instancias mediante metadatos de instancia

Para recuperar información sobre los eventos de mantenimiento activos de las instancias desde los metadatos de las instancias puede utilizar el Servicio de metadatos de instancia, versión 2, o el Servicio de metadatos de instancia, versión 1.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/events/maintenance/scheduled
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/events/maintenance/scheduled
```

A continuación se muestra un resultado de ejemplo con información acerca de un evento de reinicio del sistema programado, en formato JSON.

```
[
  {
    "NotBefore" : "21 Jan 2019 09:00:43 GMT",
    "Code" : "system-reboot",
    "Description" : "scheduled reboot",
    "EventId" : "instance-event-0d59937288b749b32",
    "NotAfter" : "21 Jan 2019 09:17:23 GMT",
    "State" : "active"
  }
]
```

Para ver el historial de los eventos completados o cancelados mediante los metadatos de las instancias

Para recuperar información sobre los eventos completados o cancelados desde las instancias de metadatos puede utilizar el Servicio de metadatos de instancia, versión 2, o el Servicio de metadatos de instancia, versión 1.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/events/maintenance/history
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/events/maintenance/history
```

A continuación se muestra un resultado de ejemplo con información acerca de un evento de reinicio del sistema que se canceló y un evento de reinicio del sistema que se completó, en formato JSON.

```
[
  {
    "NotBefore" : "21 Jan 2019 09:00:43 GMT",
    "Code" : "system-reboot",
    "Description" : "[Canceled] scheduled reboot",
    "EventId" : "instance-event-0d59937288b749b32",
    "NotAfter" : "21 Jan 2019 09:17:23 GMT",
    "State" : "canceled"
  },
  {
    "NotBefore" : "29 Jan 2019 09:00:43 GMT",
    "Code" : "system-reboot",
    "Description" : "[Completed] scheduled reboot",
    "EventId" : "instance-event-0d59937288b749b32",
    "NotAfter" : "29 Jan 2019 09:17:23 GMT",
    "State" : "completed"
  }
]
```

AWS Health

Puede usar AWS Health Dashboard para obtener información sobre eventos que pueden afectar a su instancia. En el AWS Health Dashboard, los problemas están organizados en tres grupos: problemas abiertos, cambios programados y otras notificaciones. El grupo de cambios programados contiene elementos próximos o que están en curso.

Para obtener más información, consulte Introducción a su AWS Health Dashboard en la Guía del usuario de AWS Health.

Personalizar notificaciones de eventos programados

Puede personalizar las notificaciones de eventos programados para incluir etiquetas en la notificación de correo electrónico. Esto hace que sea más fácil identificar el recurso afectado (instancias o Hosts dedicados) y priorizar acciones para el próximo evento.

Al personalizar las notificaciones de eventos para incluir etiquetas, puede elegir incluir:

- Todas las etiquetas que están asociadas con el recurso afectado
- Solo las etiquetas específicas que están asociadas con el recurso afectado

Por ejemplo, supongamos que asigna etiquetas `application`, `costcenter`, `project` y `owner` a todas las instancias. Puede elegir incluir todas las etiquetas en las notificaciones de eventos. Alternativamente, si desea ver solo las etiquetas `owner` y `project` en las notificaciones de eventos, puede elegir incluir solo esas etiquetas.

Después de seleccionar las etiquetas que se van a incluir, las notificaciones de eventos incluirán el ID de recurso (ID de instancia o ID de host dedicado) y los pares de valores y clave de etiqueta asociados al recurso afectado.

Tareas

- Incluir etiquetas en las notificaciones de eventos
- Eliminar etiquetas de las notificaciones de eventos
- Ver las etiquetas que se incluirán en las notificaciones de eventos

Incluir etiquetas en las notificaciones de eventos

Las etiquetas que elija incluir se aplican a todos los recursos (instancias y Hosts dedicados) de la región seleccionada. Para personalizar las notificaciones de eventos en otras regiones, seleccione primero la región requerida y, a continuación, realice los siguientes pasos.

Para incluir etiquetas en las notificaciones de eventos, puede utilizar uno de los siguientes métodos.

Console

Para incluir etiquetas en las notificaciones de eventos

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Events (Eventos).
3. Seleccione Actions (Acciones), Manage event notifications (Administrar notificaciones de eventos).
4. Activar Incluir etiquetas en las notificaciones de eventos.
5. Realice una de las siguientes acciones, dependiendo de las etiquetas que desee incluir en las notificaciones de eventos:
   - Para incluir todas las etiquetas asociadas a la instancia afectada o host dedicado, seleccione Incluir todas las etiquetas de recursos.
   - Para seleccionar las etiquetas que se van a incluir, seleccione Elegir las etiquetas que se van a incluir y, a continuación, seleccione o ingrese las claves de etiqueta.
6. Seleccione Guardar.

AWS CLI

Para incluir todas las etiquetas en las notificaciones de eventos

Utilice el comando register-instance-event-notification-attributes de AWS CLI y establezca el parámetro `IncludeAllTagsOfInstance` en `true`.

```
aws ec2 register-instance-event-notification-attributes \
    --instance-tag-attribute "IncludeAllTagsOfInstance=true"
```

Para incluir etiquetas específicas en las notificaciones de eventos

Utilice el comando register-instance-event-notification-attributes de AWS CLI y especifique las etiquetas que desea incluir utilizando el parámetro `InstanceTagKeys`.

```
aws ec2 register-instance-event-notification-attributes \
    --instance-tag-attribute 'InstanceTagKeys=["tag_key_1", "tag_key_2",
 "tag_key_3"]'
```

Eliminar etiquetas de las notificaciones de eventos

Para quitar etiquetas de las notificaciones de eventos, puede utilizar uno de los siguientes métodos.

Console

Para eliminar etiquetas de las notificaciones de eventos

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Events (Eventos).
3. Seleccione Actions (Acciones), Manage event notifications (Administrar notificaciones de eventos).
4. Para quitar todas las etiquetas de las notificaciones de eventos, desactive Incluir etiquetas en las notificaciones de eventos.
5. Para eliminar etiquetas específicas de las notificaciones de eventos, seleccione la X) para las claves de etiqueta correspondientes.
6. Seleccione Guardar.

AWS CLI

Para eliminar todas las etiquetas de las notificaciones de eventos

Utilice el comando deregister-instance-event-notification-attributes de AWS CLI y establezca el parámetro `IncludeAllTagsOfInstance` en `false`.

```
aws ec2 deregister-instance-event-notification-attributes \
    --instance-tag-attribute "IncludeAllTagsOfInstance=false"
```

Para eliminar etiquetas específicas de las notificaciones de eventos

Utilice el comando deregister-instance-event-notification-attributes de AWS CLI y especifique las etiquetas que desea eliminar mediante el parámetro `InstanceTagKeys`.

```
aws ec2 deregister-instance-event-notification-attributes \
    --instance-tag-attribute 'InstanceTagKeys=["tag_key_1", "tag_key_2",
 "tag_key_3"]'
```

Ver las etiquetas que se incluirán en las notificaciones de eventos

Para ver las etiquetas que se van a incluir en las notificaciones de eventos, utilice uno de los siguientes métodos.

Console

Para ver las etiquetas que se van a incluir en las notificaciones de eventos

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Events (Eventos).
3. Seleccione Actions (Acciones), Manage event notifications (Administrar notificaciones de eventos).

AWS CLI

Para ver las etiquetas que se van a incluir en las notificaciones de eventos

Utilice el comando describe-instance-event-notification-attributes de AWS CLI.

```
aws ec2 describe-instance-event-notification-attributes
```

Trabajar con instancias programadas para detener o retirar

Cuando AWS detecta un error irreparable del host subyacente de la instancia, programa la detención o terminación de la instancia, según el tipo de dispositivo raíz de la instancia. Si el dispositivo raíz es un volumen de EBS, la instancia está programada para su detención. Si el dispositivo raíz es un volumen de almacén de instancias, la instancia está programada para su terminación. Para obtener más información, consulte Retirada de instancias.

Important

Cualquier dato almacenado en volúmenes del almacén de instancias se perderá cuando una instancia se detenga, se termine o se ponga en hibernación. Esto incluye volúmenes de almacén de instancias adjuntadas a una instancia que tiene un volumen de EBS como dispositivo raíz. No olvide guardar los datos de los volúmenes del almacén de instancias que puede necesitar más adelante antes de que la instancia se detenga, se termine o se ponga en hibernación.

Acciones para instancias respaldadas por Amazon EBS

Puede esperar a que la instancia se detenga como estaba programado. Asimismo, puede detener e iniciar la instancia usted mismo, lo que hace que la instancia migre a un nuevo host. Para obtener más información acerca de cómo detener la instancia, además de información acerca de los cambios a la configuración de la instancia cuando se detiene, consulte Detención e iniciación de una instancia de Amazon EC2.

Puede automatizar la detención y el inicio inmediatos en respuesta a un evento programado para la detención de la instancia. Para obtener más información, consulte la sección Automatización de acciones en instancias de Amazon EC2 en la Guía del usuario de AWS Health.

Acciones para instancias con respaldo en el almacén de instancias

Le recomendamos que lance una instancia de sustitución desde la AMI más reciente y que migre todos los datos necesarios a la instancia de sustitución antes de la instancia que está programada para terminar. A continuación, puede terminar la instancia original o esperar a que termine como estaba programado.

Trabajar con instancias programadas para el reinicio

Cuando AWS debe realizar algunas tareas, como instalar actualizaciones o realizar el mantenimiento del host subyacente, puede programar la instancia o el host subyacente para reinicio. Puede reprogramar la mayoría de los eventos de reinicio de modo que la instancia se reinicie en la fecha y hora específica que mejor le convenga.

Ver el tipo de evento de reinicio

Para consultar si un evento de reinicio es un reinicio de instancia o un reinicio del sistema, utilice uno de los siguientes métodos.

Console

Para ver el tipo de evento de reinicio programado

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Events (Eventos).
3. Elija Resource type: instance (Tipo de recurso: instancia) en la lista de filtros.
4. Para cada instancia, consulte el valor en la columna Event Type (Tipo de evento). El valor es system-reboot o instance-reboot.

AWS CLI

Para ver el tipo de evento de reinicio programado

Utilice el comando describe-instance-status.

```
aws ec2 describe-instance-status \
    --instance-id i-1234567890abcdef0
```

Para eventos de reinicio programados, el valor de `Code` es `system-reboot` o bien `instance-reboot`. La siguiente salida de ejemplo muestra un evento `system-reboot`.

```
[
    "Events": [
                {
                    "InstanceEventId": "instance-event-0d59937288b749b32",
                    "Code": "system-reboot",
                    "Description": "The instance is scheduled for a reboot",
                    "NotAfter": "2019-03-14T22:00:00.000Z",
                    "NotBefore": "2019-03-14T20:00:00.000Z",
                    "NotBeforeDeadline": "2019-04-05T11:00:00.000Z"
                }
            ]
]
```

Acciones para reinicio de instancias

Puede esperar a que se produzca el reinicio de la instancia en su periodo de mantenimiento programado, reprogramar el reinicio de la instancia a la fecha y hora que mejor le convenga o reiniciar la instancia usted mismo a una hora que le resulte práctica.

Después de reiniciar la instancia, el evento programado se elimina y se actualiza la descripción del evento. Se ha completado el mantenimiento pendiente del host subyacente y puede empezar a usar la instancia de nuevo después de que se haya reiniciado completamente.

Acciones para reinicio de sistemas

No puede reiniciar el sistema usted mismo. Puede esperar a que se produzca el reinicio del sistema durante su periodo de mantenimiento programado o puede reprogramar el reinicio del sistema a la fecha y hora que mejor le convenga. Un reinicio del sistema se suele completar en unos pocos minutos. Una vez que ha tenido lugar el reinicio del sistema, la instancia retiene su dirección IP y

nombre de DNS, y se conservan todos los datos en los volúmenes del almacén de instancias local. Después de que se complete el reinicio del sistema, se borra el evento programado para la instancia y puede verificar que el software de la instancia está funcionando tal como se espera.

Asimismo, si es necesario realizar el mantenimiento de la instancia a otra hora y no puede reprogramar el reinicio del sistema, entonces puede detener e iniciar una instancia respaldada por Amazon EBS, lo que hará que migre a un nuevo host. No obstante, los datos en los volúmenes de almacén de instancias local no se conservarán. También puede automatizar la detención y el inicio inmediatos de la instancia en respuesta a un evento programado para reiniciar el sistema. Para obtener más información, consulte la información sobre la Automatización de acciones en instancias de EC2 en la Guía del usuario de AWS Health. Para una instancia respaldada por un almacén de instancias, si no puede reprogramar el reinicio del sistema, entonces puede lanzar una instancia de sustitución desde la AMI más reciente, migrar todos los datos necesarios a la instancia de sustitución antes del periodo de mantenimiento programado y terminar la instancia original.

Trabajar con instancias programadas para mantenimiento

Cuando AWS debe realizar el mantenimiento del host subyacente de una instancia, programa la instancia para su mantenimiento. Existen dos tipos de eventos de mantenimiento: mantenimiento de red y mantenimiento de energía.

Durante el mantenimiento de red, las instancias programadas pierden la conectividad de red durante un breve periodo de tiempo. La conectividad de red normal a la instancia se restaurará una vez completado el mantenimiento.

Durante el mantenimiento de energía, las instancias programadas se desconectan durante un breve periodo y, a continuación, se reinician. Cuando se realiza un reinicio, se conservan todos los valores de configuración de la instancia.

Una vez reiniciada la instancia (esto normalmente tarda unos minutos), verifique que su aplicación está funcionando tal como se espera. En este momento, la instancia ya no debería tener un evento programado asociado o si lo tuviese, la descripción del evento programado empezaría con [Completed] (Finalizado). A veces, se tarda hasta 1 hora en actualizar la descripción de estado de la instancia. Los eventos de mantenimiento completados se muestran en el panel de la consola de Amazon EC2 durante una semana.

Acciones para instancias respaldadas por Amazon EBS

Puede esperar a que el mantenimiento suceda tal como estaba programado. Asimismo, puede detener e iniciar la instancia, lo que hará que migre a un nuevo host. Para obtener más información

acerca de cómo detener la instancia, además de información acerca de los cambios a la configuración de la instancia cuando se detiene, consulte Detención e iniciación de una instancia de Amazon EC2.

Puede automatizar la detención y el inicio inmediatos en respuesta a un evento de mantenimiento programado. Para obtener más información, consulte la información sobre la Automatización de acciones en instancias de EC2 en la Guía del usuario de AWS Health.

Acciones para instancias con respaldo en el almacén de instancias

Puede esperar a que el mantenimiento suceda tal como estaba programado. Asimismo, si desea mantener el funcionamiento normal durante un periodo de mantenimiento programado, puede lanzar una instancia de sustitución desde la AMI más reciente, migrar todos los datos necesarios a la instancia de sustitución antes del periodo de mantenimiento programado y, a continuación, terminar la instancia original.

Reprogramar un evento programado

Puede reprogramar un evento para que se produzca en la fecha y hora específicas que mejor le convenga. Solo se pueden reprogramar los eventos que tienen una fecha límite. Existen otras limitaciones para reprogramar un evento.

Para reprogramar un evento, utilice uno de los siguientes métodos.

Console

Para reprogramar un evento

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Events (Eventos).
3. Elija Resource type: instance (Tipo de recurso: instancia) en la lista de filtros.
4. Seleccione una o varias instancias y, a continuación, elija Actions (Acciones), Schedule Event (Programar evento).

   Solo se pueden reprogramar los eventos que tienen una fecha límite de evento indicada por un valor de Deadline (Fecha límite). Si uno de los eventos seleccionados no tiene fecha límite, Actions (Acciones) y Schedule event (Programar evento) están deshabilitados.
5. En New start time (Nueva hora de inicio), escriba una nueva fecha y hora para el evento. La nueva fecha y hora deben ser anteriores al valor especificado en Event deadline (Fecha límite de evento).

6. Seleccione Guardar.

   La hora de inicio del evento actualizada podría tardar uno o dos minutos en reflejarse en la consola.

AWS CLI

Para reprogramar un evento

1. Solo se pueden reprogramar los eventos que tienen una fecha límite de evento, indicada por un valor en `NotBeforeDeadline`. Utilice el comando describe-instance-status para consultar el valor del parámetro `NotBeforeDeadline`.

```
aws ec2 describe-instance-status \
    --instance-id i-1234567890abcdef0
```

   La siguiente salida de ejemplo muestra un evento `system-reboot` que se puede reprogramar dado que `NotBeforeDeadline` contiene un valor.

```
[
    "Events": [
                {
                    "InstanceEventId": "instance-event-0d59937288b749b32",
                    "Code": "system-reboot",
                    "Description": "The instance is scheduled for a reboot",
                    "NotAfter": "2019-03-14T22:00:00.000Z",
                    "NotBefore": "2019-03-14T20:00:00.000Z",
                    "NotBeforeDeadline": "2019-04-05T11:00:00.000Z"
                }
              ]
]
```

2. Para reprogramar el evento, utilice el comando modify-instance-event-start-time. Para especificar la nueva hora de inicio del evento, utilice el parámetro `not-before`. La nueva hora de inicio del evento debe ser anterior al `NotBeforeDeadline`.

```
aws ec2 modify-instance-event-start-time \
    --instance-id i-1234567890abcdef0 \
    --instance-event-id instance-event-0d59937288b749b32 \
    --not-before 2019-03-25T10:00:00.000
```

Podrían pasar uno o dos minutos hasta que el comando describe-instance-status devuelva el valor de parámetro `not-before` actualizado.

Limitaciones

- Solo se pueden reprogramar los eventos con una fecha límite de evento. El evento se puede reprogramar hasta la fecha límite del evento. La columna Deadline (Fecha límite) en la consola y el campo `NotBeforeDeadline` en la AWS CLI indican si el evento tiene una fecha límite.
- Solo se pueden reprogramar los eventos que no se han iniciado aún. La columna Start time (Hora de inicio) en la consola y el campo `NotBefore` en la AWS CLI indican la hora de inicio del evento. Los eventos que se han programado para comenzar en los siguientes cinco minutos no se pueden reprogramar.
- La nueva hora de inicio del evento debe comenzar al menos 60 minutos a partir de la hora actual.
- Si reprograma múltiples eventos utilizando la consola, la fecha límite del evento se determina por el evento con la fecha límite de evento más temprana.

Definir periodos de eventos para eventos programados

Puede definir ventanas de eventos semanales personalizados para eventos programados que reinicien, detengan o terminen sus instancias de Amazon EC2. Puede asociar una o varias instancias con un periodo de evento. Si se planifica un evento programado para esas instancias, AWS programará los eventos dentro del periodo de eventos asociado.

Puede utilizar los periodos de eventos para maximizar la disponibilidad de la carga de trabajo mediante la especificación de los periodos de eventos que se producen durante los periodos de menor actividad de su carga de trabajo. También puede alinear los periodos de eventos con sus programas de mantenimiento internos.

Define un periodo de evento mediante la especificación de un conjunto de intervalos de tiempo. El intervalo de tiempo mínimo es de 2 horas. Los intervalos de tiempo combinados deben sumar como mínimo 4 horas.

Puede asociar una o varias instancias con un periodo de evento mediante ID de instancia o etiquetas de instancia. También puede asociar host dedicados con periodos de eventos mediante el ID de alojamiento.

> **Warning**
>
> Los periodos de eventos solo se aplican a eventos programados que detienen, reinician o terminan instancias.
> Los periodos de eventos no se aplican a lo siguiente:
>
> - eventos programados rápidos y eventos de mantenimiento de red
> - mantenimiento no programado, como AutoRecovery y reinicios no planificados

Trabajar con periodos de eventos

- Consideraciones
- Ver periodos de eventos
- Crear periodos de eventos
- Modificar periodos de eventos
- Eliminar periodos de eventos
- Etiquetar periodos de eventos

Consideraciones

- Las horas de los periodos de eventos se indican en UTC.
- La duración mínima de la ventana de evento semanal es de 4 horas.
- Los intervalos de tiempo dentro de un periodo de evento deben ser de 2 horas como mínimo.
- Solo se puede asociar un tipo de destino (ID de instancia, ID de host dedicado o etiqueta de instancia) con un periodo de evento.
- Un destino (ID de instancia, ID de host dedicado o etiqueta de instancia) solo se puede asociar con un periodo de evento.
- Se puede asociar un máximo de 100 ID de instancia, 50 ID de host dedicado o 50 etiquetas de instancia con un periodo de evento. Las etiquetas de instancia pueden asociarse con cualquier cantidad de instancias.
- Se puede crear un máximo de 200 periodos de eventos por región de AWS.
- Es posible que varias instancias asociadas con periodos de eventos tengan eventos programados que ocurran al mismo tiempo.

- Si AWS ya ha programado un evento, la modificación de un periodo de evento no cambiará el horario del evento programado. Si el evento tiene una fecha límite, puede reprogramar el evento.
- Puede detener e iniciar una instancia antes del evento programado, por lo que se migra la instancia a un nuevo host, de manera que el evento programado ya no se llevará a cabo.

Ver periodos de eventos

Para ver los periodos de eventos, utilice uno de los siguientes métodos.

Console

Para ver periodos de eventos

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Events (Eventos).
3. Elija Actions (Acciones), Manage event windows (Administrar periodos de eventos).
4. Seleccione un periodo de evento para ver los detalles.

AWS CLI

Para describir todos los periodos de eventos

Utilice el comando describe-instance-event-windows.

```
aws ec2 describe-instance-event-windows \
    --region us-east-1
```

Salida prevista

```
{
    "InstanceEventWindows": [
        {
            "InstanceEventWindowId": "iew-0abcdef1234567890",
            "Name": "myEventWindowName",
            "CronExpression": "* 21-23 * * 2,3",
            "AssociationTarget": {
                "InstanceIds": [
                    "i-1234567890abcdef0",
```

```
                    "i-0598c7d356eba48d7"
                ],
                "Tags": [],
                "DedicatedHostIds": []
            },
            "State": "active",
            "Tags": []
        }

        ...

    ],
    "NextToken": "9d624e0c-388b-4862-a31e-a85c64fc1d4a"
}
```

Para describir un periodo de evento específico

Utilice el comando describe-instance-event-windows con el parámetro `--instance-event-window-id` para describir un periodo de evento específico.

```
aws ec2 describe-instance-event-windows \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890
```

Para describir los periodos de eventos que coinciden con uno o varios filtros

Utilice el comando describe-instance-event-windows con el parámetro `--filters`. En el siguiente ejemplo, el filtro `instance-id` se utiliza para describir todas las ventanas de eventos asociadas con la instancia especificada.

Cuando se utiliza un filtro, este realiza una coincidencia directa. Sin embargo, el filtro `instance-id` es diferente. Si no hay una coincidencia directa con el ID de instancia, se recurre a asociaciones indirectas con el periodo de evento, como las etiquetas de la instancia o el ID de host dedicado (si la instancia está en un host dedicado).

Para obtener la lista de filtros admitidos, consulte describe-instance-event-windows en la Referencia de la AWS CLI.

```
aws ec2 describe-instance-event-windows \
    --region us-east-1 \
    --filters Name=instance-id,Values=i-1234567890abcdef0 \
```

```
    --max-results 100 \
    --next-token <next-token-value>
```

Salida prevista

En el siguiente ejemplo, la instancia se encuentra en un host dedicado, que está asociado con el periodo de evento.

```
{
    "InstanceEventWindows": [
        {
            "InstanceEventWindowId": "iew-0dbc0adb66f235982",
            "TimeRanges": [
                {
                    "StartWeekDay": "sunday",
                    "StartHour": 2,
                    "EndWeekDay": "sunday",
                    "EndHour": 8
                }
            ],
            "Name": "myEventWindowName",
            "AssociationTarget": {
                "InstanceIds": [],
                "Tags": [],
                "DedicatedHostIds": [
                    "h-0140d9a7ecbd102dd"
                ]
            },
            "State": "active",
            "Tags": []
        }
    ]
}
```

Crear periodos de eventos

Puede crear uno o varios periodos de eventos. Para cada periodo de evento, debe especificar uno o varios bloques de tiempo. Por ejemplo, puede crear una ventana de evento con bloques de tiempo que ocurran todos los días a las 4 h durante 2 horas. También puede crear una ventana de evento con bloques de tiempo que ocurran los domingos entre las 2 h y las 4 h y los miércoles entre las 3 h y las 5 h.

Para conocer las restricciones de los periodos de eventos, consulte Consideraciones que aparece antes en este tema.

Los periodos de eventos se repiten semanalmente hasta que se eliminan.

Utilice uno de los siguientes métodos para crear un periodo de evento.

Console

Para crear un periodo de evento

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Events (Eventos).
3. Elija Actions (Acciones), Manage event windows (Administrar periodos de eventos).
4. Seleccione Create instance event window (Crear periodo de evento de instancia).
5. En Event window name (Nombre del periodo de evento), ingrese un nombre descriptivo para el periodo de evento.
6. En Event window schedule (Programación del periodo de evento), elija especificar los bloques de tiempo en el periodo de evento con el generador de programación cron o mediante la especificación de los intervalos de tiempo.

   - Si elige Cron schedule builder (Generador de programación cron), especifique lo siguiente:
     1. En Days (UTC) (Días [UTC]), especifique los días de la semana en los que ocurrirá el periodo de evento.
     2. En Start time (UTC) (Hora de inicio [UTC]), especifique la hora a la que comenzará el periodo de evento.
     3. En Duration (Duración), especifique la duración de los bloques de tiempo del periodo de evento. La duración mínima por bloque de tiempo es de 2 horas. La duración mínima del periodo de evento debe ser igual o superior a 4 horas en total. Todas las horas se indican en UTC.
   - Si elige Time ranges (Intervalos de tiempo), elija Add new time range (Agregar un intervalo de tiempo nuevo) y especifique el día y la hora de inicio y el día y la hora de finalización. Repita este procedimiento para cada intervalo de tiempo. La duración mínima por intervalo de tiempo es de 2 horas. La duración mínima para todos los intervalos de tiempo combinados debe ser igual o superior a 4 horas en total.
7. (Opcional) En Target details (Detalles del destino), asocie una o varias instancias con el periodo de evento de manera que si las instancias están programadas para mantenimiento,

el evento programado ocurrirá durante el periodo de evento asociado. Para asociar una o varias instancias con una ventana de evento, utilice ID de instancia o etiquetas de instancia. Para asociar host dedicados con ventanas de eventos, utilice el ID de host.

Tenga en cuenta que puede crear ventanas de eventos sin asociar un destino al la ventana. Luego, puede modificar el periodo para asociar uno o más destinos.

8. (Opcional) En Event window tags (Etiquetas del periodo de evento), elija Add tag (Agregar etiqueta) e ingrese la clave y el valor de la etiqueta. Repita este proceso para cada etiqueta.
9. Elija Create event window (Crear un periodo de evento).

AWS CLI

Para crear una ventana de evento mediante la AWS CLI, primero debe crear la ventana de evento y, luego, asociarla con uno o más destinos.

Crear un periodo de evento

Cuando crea un periodo de evento, puede definir un conjunto de intervalos de tiempo o una expresión cron, pero no ambos.

Para crear un periodo de evento con un intervalo de tiempo

Utilice el comando create-instance-event-window y especifique el parámetro `--time-range`. No puede especificar el parámetro `--cron-expression`.

```
aws ec2 create-instance-event-window \
    --region us-east-1 \
    --time-range StartWeekDay=monday,StartHour=2,EndWeekDay=wednesday,EndHour=8 \
    --tag-specifications "ResourceType=instance-event-
window,Tags=[{Key=K1,Value=V1}]" \
    --name myEventWindowName
```

Resultado previsto

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "TimeRanges": [
            {
```

```
                "StartWeekDay": "monday",
                "StartHour": 2,
                "EndWeekDay": "wednesday",
                "EndHour": 8
            }
        ],
        "Name": "myEventWindowName",
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

Para crear un periodo de evento con una expresión cron

Utilice el comando create-instance-event-window y especifique el parámetro `--cron-expression`. No puede especificar el parámetro `--time-range`.

```
aws ec2 create-instance-event-window \
    --region us-east-1 \
    --cron-expression "* 21-23 * * 2,3" \
    --tag-specifications "ResourceType=instance-event-
window,Tags=[{Key=K1,Value=V1}]" \
    --name myEventWindowName
```

Salida prevista

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
```

```
        ]
    }
}
```

Asociar un destino con un periodo de evento

Solo se puede asociar un tipo de destino (ID de instancia, ID de host dedicado o etiquetas de instancia) con un periodo de evento.

Para asociar las etiquetas de instancia con un periodo de evento

Utilice el comando associate-instance-event-window y especifique el parámetro `instance-event-window-id` para determinar el periodo de evento. Para asociar las etiquetas de instancia, especifique el parámetro `--association-target`, y para los valores del parámetro, especifique una o varias etiquetas.

```
aws ec2 associate-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceTags=[{Key=k2,Value=v2},{Key=k1,Value=v1}]"
```

Resultado previsto

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [
                {
                    "Key": "k2",
                    "Value": "v2"
                },
                {
                    "Key": "k1",
                    "Value": "v1"
                }
            ],
            "DedicatedHostIds": []
        },
```

```
        "State": "creating"
    }
}
```

Para asociar una o varias instancias con un periodo de evento

Utilice el comando associate-instance-event-window y especifique el parámetro `instance-event-window-id` para determinar el periodo de evento. Para asociar instancias, especifique el parámetro `--association-target`, y para los valores del parámetro, especifique uno o varios ID de instancia.

```
aws ec2 associate-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceIds=i-1234567890abcdef0,i-0598c7d356eba48d7"
```

Resultado previsto

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [
                "i-1234567890abcdef0",
                "i-0598c7d356eba48d7"
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

Para asociar un host dedicado con un periodo de evento

Utilice el comando associate-instance-event-window y especifique el parámetro `instance-event-window-id` para determinar el periodo de evento. Para asociar un host dedicado, especifique el parámetro `--association-target`, y para los valores del parámetro, especifique uno o varios ID de alojamiento dedicado.

```
aws ec2 associate-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "DedicatedHostIds=h-029fa35a02b99801d"
```

Salida prevista

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
            "DedicatedHostIds": [
                "h-029fa35a02b99801d"
            ]
        },
        "State": "creating"
    }
}
```

Modificar periodos de eventos

Puede modificar todos los campos de una ventana de evento excepto su ID. Por ejemplo, es posible que desee modificar la programación del periodo de evento cuando comience el horario de verano. Es posible que desee agregar o eliminar destinos para los periodos de eventos existentes.

Utilice uno de los siguientes métodos para modificar un periodo de evento.

Console

Para modificar un periodo de evento

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Events (Eventos).
3. Elija Actions (Acciones), Manage event windows (Administrar periodos de eventos).
4. Seleccione el periodo de evento que desea modificar y, luego, elija Actions (Acciones), Modify instance event window (Modificar periodo de evento de instancia).

5. Modifique los campos del periodo de evento y, luego, elijaModify event window (Modificar periodo de evento).

AWS CLI

Para modificar un periodo de evento mediante la AWS CLI, se puede modificar el intervalo de tiempo o la expresión cron, y asociar uno o varios destinos con el periodo de evento o desasociarlos de este.

Modificar la hora del periodo de evento

Cuando modifica el periodo de evento, puede modificar un intervalo de tiempo o una expresión cron, pero no ambos.

Para modificar el intervalo de tiempo de un periodo de evento

Utilice el comando modify-instance-event-window y especifique el periodo de evento que se modificará. Especifique el parámetro `--time-range` para modificar el intervalo de tiempo. No puede especificar el parámetro `--cron-expression`.

```
aws ec2 modify-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --time-range StartWeekDay=monday,StartHour=2,EndWeekDay=wednesday,EndHour=8
```

Resultado previsto

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "TimeRanges": [
            {
                "StartWeekDay": "monday",
                "StartHour": 2,
                "EndWeekDay": "wednesday",
                "EndHour": 8
            }
        ],
        "Name": "myEventWindowName",
        "AssociationTarget": {
            "InstanceIds": [
```

```
                "i-0abcdef1234567890",
                "i-0be35f9acb8ba01f0"
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

Para modificar un conjunto de intervalos de tiempo para un periodo de evento

Utilice el comando modify-instance-event-window y especifique el periodo de evento que se modificará. Especifique el parámetro `--time-range` para modificar el intervalo de tiempo. No se puede especificar el parámetro `--cron-expression` en la misma llamada.

```
aws ec2 modify-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --time-range '[{"StartWeekDay": "monday", "StartHour": 2, "EndWeekDay":
 "wednesday", "EndHour": 8},
   {"StartWeekDay": "thursday", "StartHour": 2, "EndWeekDay": "friday",
 "EndHour": 8}]'
```

Resultado previsto

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "TimeRanges": [
            {
                "StartWeekDay": "monday",
                "StartHour": 2,
                "EndWeekDay": "wednesday",
                "EndHour": 8
            },
```

```
            {
                "StartWeekDay": "thursday",
                "StartHour": 2,
                "EndWeekDay": "friday",
                "EndHour": 8
            }
        ],
        "Name": "myEventWindowName",
        "AssociationTarget": {
            "InstanceIds": [
                "i-0abcdef1234567890",
                "i-0be35f9acb8ba01f0"
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

Para modificar la expresión cron de un periodo de evento

Utilice el comando modify-instance-event-window y especifique el periodo de evento que se modificará. Especifique el parámetro `--cron-expression` para modificar la expresión cron. No puede especificar el parámetro `--time-range`.

```
aws ec2 modify-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --cron-expression "* 21-23 * * 2,3"
```

Salida prevista

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
```

```
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [
                "i-0abcdef1234567890",
                "i-0be35f9acb8ba01f0"
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

Modificar los destinos asociados con un periodo de evento

Puede asociar destinos adicionales con un periodo de evento. También puede desasociar destinos existentes de un periodo de evento. Sin embargo, solo se puede asociar un tipo de destino (ID de instancia, ID de host dedicado o etiquetas de instancia) con un periodo de evento.

Para asociar destinos adicionales con un periodo de evento

Para obtener instrucciones sobre cómo asociar destinos con un periodo de evento, consulte Associate a target with an event window.

Para desasociar las etiquetas de instancia de un periodo de evento

Utilice el comando disassociate-instance-event-window y especifique el parámetro `instance-event-window-id` para determinar el periodo de evento. Para desasociar las etiquetas de instancia, especifique el parámetro `--association-target`, y para los valores del parámetro, especifique una o varias etiquetas.

```
aws ec2 disassociate-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceTags=[{Key=k2,Value=v2},{Key=k1,Value=v1}]"
```

Resultado previsto

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

Para desasociar una o varias instancias de un periodo de evento

Utilice el comando disassociate-instance-event-window y especifique el parámetro `instance-event-window-id` para determinar el periodo de evento. Para desasociar instancias, especifique el parámetro `--association-target`, y para los valores del parámetro, especifique uno o varios ID de instancia.

```
aws ec2 disassociate-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceIds=i-1234567890abcdef0,i-0598c7d356eba48d7"
```

Resultado previsto

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
```

```
}
```

Para desasociar un host dedicado de un periodo de evento

Utilice el comando disassociate-instance-event-window y especifique el parámetro `instance-event-window-id` para determinar el periodo de evento. Para desasociar un host dedicado, especifique el parámetro `--association-target`, y para los valores del parámetro, especifique uno o varios ID de alojamiento dedicado.

```
aws ec2 disassociate-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target DedicatedHostIds=h-029fa35a02b99801d
```

Salida prevista

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

Eliminar periodos de eventos

Para eliminar una ventana de evento a la vez, utilice uno de los siguientes métodos.

Console

Para eliminar un periodo de evento

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Events (Eventos).

3. Elija Actions (Acciones), Manage event windows (Administrar periodos de eventos).
4. Seleccione el periodo de evento que desea eliminar y, luego, elija Actions (Acciones), Delete instance event window (Eliminar periodo de evento de instancia).
5. Cuando se le pregunte, escriba **`delete`** y, a continuación, elija Delete (Eliminar).

AWS CLI

Para eliminar un periodo de evento

Utilice el comando delete-instance-event-window y especifique el periodo de evento que se eliminará.

```
aws ec2 delete-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890
```

Para forzar la eliminación de un periodo de evento

Utilice el parámetro `--force-delete` si el periodo de evento está asociado actualmente con los destinos.

```
aws ec2 delete-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --force-delete
```

Salida prevista

```
{
    "InstanceEventWindowState": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "State": "deleting"
    }
}
```

Etiquetar periodos de eventos

Puede etiquetar un periodo de evento en el momento de su creación o después.

Para etiquetar un periodo de evento en el momento de la creación, consulte Crear periodos de eventos.

Utilice uno de los siguientes métodos para etiquetar un periodo de evento.

Console

Para etiquetar un periodo de evento existente

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Events (Eventos).
3. Elija Actions (Acciones), Manage event windows (Administrar periodos de eventos).
4. Seleccione el periodo de evento que desea etiquetar y, luego, elija Actions (Acciones), Manage instance event window tags (Administrar etiquetas del periodo de evento de instancia).
5. Para agregar una etiqueta, elija Add tag (Agregar etiqueta). Repita este proceso para cada etiqueta.
6. Seleccione Guardar.

AWS CLI

Para etiquetar un periodo de evento existente

Utilice el comando create-tags para etiquetar recursos existentes. En el siguiente ejemplo, el periodo de evento existente se etiqueta con Key=purpose y Value=test.

```
aws ec2 create-tags \
    --resources iew-0abcdef1234567890 \
    --tags Key=purpose,Value=test
```

Monitorear las instancias con CloudWatch

Puede monitorizar las instancias mediante Amazon CloudWatch, que recopila y procesa los datos sin formato de Amazon EC2 y los convierte en métricas legibles prácticamente en tiempo real. Estas estadísticas se registran durante un periodo de 15 meses, de forma que pueda obtener acceso a información de historial y obtener una mejor perspectiva acerca del desempeño de su aplicación web o servicio.

De forma predeterminada, Amazon EC2 envía los datos de las métricas a CloudWatch en periodos de 5 minutos. Para enviar los datos de las métricas de la instancia a CloudWatch en periodos de 1 minuto, puede habilitar un monitoreo detallado para la instancia. Para obtener más información, consulte Activar o desactivar el monitoreo detallado para las instancias.

La consola de Amazon EC2 muestra una serie de gráficos basados en los datos sin formato de Amazon CloudWatch. En función de sus necesidades, es posible que prefiera obtener los datos de las instancias de Amazon CloudWatch en lugar de los gráficos que se muestran en la consola.

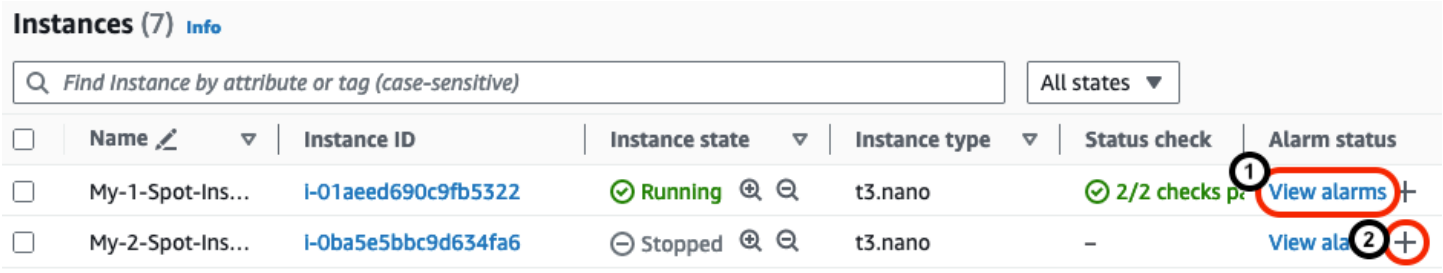
Para obtener información sobre facturación y costos de Amazon CloudWatch, consulte Facturación y costo de CloudWatch en la Guía del usuario de Amazon CloudWatch.

Contenido

Alarmas de instancias de Amazon EC2

Puede ver y crear alarmas de Amazon CloudWatch para las instancias en la pantalla Instancias de la consola de Amazon EC2.

En la siguiente captura de pantalla, se muestran los controles de la consola, numerados 1 y 2, para ver y crear alarmas desde la pantalla Instancias.



Ver alarmas desde la pantalla Instancias

Puede ver las alarmas de cada instancia desde la pantalla Instancias.

Para ver la alarma de una instancia desde la pantalla Instancias

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. En la tabla Instancias, para la instancia que elija, seleccione Ver alarmas (numeradas con 1 en la captura de pantalla anterior).
4. En la ventana Detalles de la alarma para ***i-0123456789example***, elija el nombre de la alarma para verla en la consola de CloudWatch.

Crear alarmas desde la pantalla Instancias

Puede crear una alarma para cada instancia desde la pantalla Instancias.

Para crear una alarma para una instancia desde la pantalla Instancias

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. En la tabla Instancias, para la instancia que elija, seleccione el signo más (numerado con 2 en la captura de pantalla anterior).
4. En la pantalla Administrar alarmas de CloudWatch, cree su alarma. Para obtener más información, consulte Crear una alarma de CloudWatch para una instancia.

Activar o desactivar el monitoreo detallado para las instancias

De forma predeterminada, la instancia tiene habilitada la supervisión básica. Opcionalmente, puede habilitar la supervisión detallada.

En la siguiente tabla se destacan las diferencias entre la supervisión básica y la supervisión detallada de las instancias.

Tipo de monitoreo	Descripción	Cargos
Supervisión básica	Solo las métricas de comprobación de estado están disponibles en periodos de 1 minuto. Todas las demás métricas están disponibles en periodos de 5 minutos.	Gratuito.
Supervisión detallada	Todas las métricas, incluidas las de comprobación de estado, están disponibles en periodos de 1 minuto. Para obtener este nivel de datos, debe habilitarlo específicamente para la instancia. En las instancias en las que ha habilitado el monitoreo detallado, también puede obtener datos agregados para grupos de instancias similares.	Se le cobrará por métrica que se envíe a CloudWatch. No se le cobrará por el almacenamiento de datos. Para obtener más información, consulte Paid tier (Nivel de pago) y Example 1 - EC2 Detailed Monitoring (Ejemplo 1 - Monitoreo detallado de EC2) en la página de precios de Amazon CloudWatch.

Temas

Permisos de IAM necesarios

Para habilitar la supervisión detallada de una instancia, el usuario debe tener permiso para utilizar la acción de la API MonitorInstances. Para desactivar la supervisión detallada de una instancia, el usuario debe tener permiso para usar la acción de la API UnmonitorInstances.

Habilitar el monitoreo detallado

Puede habilitar el monitoreo detallado para una instancia en el momento de lanzarla o bien una vez que la instancia está en ejecución o se detiene. Habilitar el monitoreo detallado en una instancia no afecta a la monitorización de los volúmenes de EBS asociados a la instancia. Para obtener más información, consulte Métricas de Amazon CloudWatch para Amazon EBS.

Console

Para habilitar el monitoreo detallado para una instancia existente

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Seleccione la instancia y elija Acciones, Monitoreo y solución de problemas, Administrar el monitoreo detallado.
4. En la página de detalles Detailed monitoring (Monitoreo detallado), en Detailed monitoring (Monitoreo detallado), seleccione la casilla de verificación Enable (Habilitar).
5. Seleccione Save (Guardar).

Para habilitar la monitorización detallada al lanzar una instancia

Al lanzar una instancia mediante la consola de Amazon EC2, en Detalles avanzados, seleccione la casilla de verificación Supervisión detallada de CloudWatch.

AWS CLI

Para habilitar el monitoreo detallado para una instancia existente

Utilice el siguiente comando monitor-instances para habilitar la monitorización detallada de las instancias especificadas.

```
aws ec2 monitor-instances --instance-ids i-1234567890abcdef0
```

Para habilitar la monitorización detallada al lanzar una instancia

Utilice el comando run-instances con la marca `--monitoring` para habilitar la monitorización detallada.

```
aws ec2 run-instances --image-id ami-09092360 --monitoring Enabled=true...
```

Desactivar el monitoreo detallado

Puede desactivar el monitoreo detallado en una instancia en el momento de lanzarla o bien una vez que la instancia está en ejecución o se detenga.

Console

Para desactivar la monitorización detallada

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Seleccione la instancia y elija Acciones, Monitoreo y solución de problemas, Administrar el monitoreo detallado.
4. En la página de detalles Detailed monitoring (Monitoreo detallado), en Detailed monitoring (Monitoreo detallado), desactive la casilla de verificación Enable (Habilitar).
5. Seleccione Save (Guardar).

AWS CLI

Para desactivar el monitoreo detallado

Utilice el siguiente comando unmonitor-instances para desactivar el monitoreo detallado de las instancias especificadas.

```
aws ec2 unmonitor-instances --instance-ids i-1234567890abcdef0
```

Mostrar las métricas de CloudWatch disponibles para las instancias

Amazon EC2 envía métricas a Amazon CloudWatch. Puede usar la AWS Management Console, la AWS CLI o una API para obtener una lista de las métricas que Amazon EC2 envía a CloudWatch. De forma predeterminada, cada punto de datos abarca los 5 minutos que siguen a la hora de inicio de actividad de la instancia. Si ha habilitado el monitoreo detallado, cada punto de datos abarca el siguiente minuto de actividad desde la hora de inicio. Tenga en cuenta que para las estadísticas

Mínimo, Máximo y Promedio, la granularidad mínima de las métricas que proporciona EC2 es de 1 minuto.

Para obtener más información sobre cómo recibir las estadísticas de estas métricas, consulte Obtener estadísticas para métricas de las instancias.

Contenido

Métricas de la instancia

El espacio de nombres `AWS/EC2` incluye las siguientes métricas de instancias.

Métrica	Descripción	Unidad	Estadísticas significativas
`CPUUtilization`	El porcentaje de tiempo de CPU física que Amazon EC2 utiliza para ejecutar la instancia de EC2, que incluye el tiempo dedicado a ejecutar tanto el código de usuario como el código de Amazon EC2. A muy alto nivel, `CPUUtilization` es la suma de la `CPUUtilization` de invitado y la `CPUUtilization` de hipervisor.	Porcentaje	• Media • Mínimo • Máximo

Métrica	Descripción	Unidad	Estadísticas significativas
	Las herramientas de su sistema operativo pueden mostrar un porcentaje diferente al de CloudWatch debido a factores como la simulación de dispositivos heredados, la configuración de dispositivos no heredados, las cargas de trabajo con muchas interrupciones, la migración en vivo y la actualización en vivo.		
`DiskReadOps`	Operaciones de lectura completadas de todos los volúmenes del almacén de instancias disponibles para la instancia en un periodo de tiempo especificado. Para calcular el promedio de operaciones de E/S por segundo (IOPS) para el periodo, divida el total de operaciones del periodo por el número de segundos de ese periodo. Si no hay volúmenes en el almacén de instancias, el valor es 0 o la métrica no se registra.	Recuento	• Sum • Media • Mínimo • Máximo
`DiskWriteOps`	Operaciones de escritura completadas en todos los volúmenes del almacén de instancias disponibles para la instancia en un periodo de tiempo especificado. Para calcular el promedio de operaciones de E/S por segundo (IOPS) para el periodo, divida el total de operaciones del periodo por el número de segundos de ese periodo. Si no hay volúmenes en el almacén de instancias, el valor es 0 o la métrica no se registra.	Recuento	• Sum • Media • Mínimo • Máximo

Métrica	Descripción	Unidad	Estadísticas significativas
`DiskReadBytes`	Bytes leídos de todos los volúmenes del almacén de instancias disponibles para la instancia. Esta métrica se usa para determinar el volumen de datos que la aplicación lee del disco duro de la instancia. Se puede usar para determinar la velocidad de la aplicación. El número registrado es el número de bytes recibidos durante el periodo. Si utiliza el monitoreo básico (5 minutos), puede dividir este número por 300 para conocer los bytes por segundo. Si utiliza el monitoreo detallado (1 minuto), divídalo por 60. También puede usar la función matemática métrica `DIFF_TIME` de CloudWatch para encontrar los bytes por segundo. Por ejemplo, si ha graficado `DiskReadBytes` en CloudWatch como `m1`, la fórmula matemática de métrica `m1/(DIFF_TIME(m1))` devuelve la métrica en bytes/segundo. Para obtener más información sobre `DIFF_TIME` y otras funciones matemáticas de métricas, consulte Uso de matemáticas de métricas en la Guía del usuario de Amazon CloudWatch. Si no hay volúmenes en el almacén de instancias, el valor es 0 o la métrica no se registra.	Bytes	• Sum • Media • Mínimo • Máximo

Métrica	Descripción	Unidad	Estadísticas significativas
`DiskWriteBytes`	Bytes escritos en todos los volúmenes del almacén de instancias disponibles para la instancia. Esta métrica se usa para determinar el volumen de datos que la aplicación escribe en el disco duro de la instancia. Se puede usar para determinar la velocidad de la aplicación. El número registrado es el número de bytes recibidos durante el periodo. Si utiliza el monitoreo básico (5 minutos), puede dividir este número por 300 para conocer los bytes por segundo. Si utiliza el monitoreo detallado (1 minuto), divídalo por 60. También puede usar la función matemática métrica `DIFF_TIME` de CloudWatch para encontrar los bytes por segundo. Por ejemplo, si ha graficado `DiskWriteBytes` en CloudWatch como `m1`, la fórmula matemática de métrica `m1/(DIFF_TIME(m1))` devuelve la métrica en bytes/segundo. Para obtener más información sobre `DIFF_TIME` y otras funciones matemáticas de métricas, consulte Uso de matemáticas de métricas en la Guía del usuario de Amazon CloudWatch. Si no hay volúmenes en el almacén de instancias, el valor es 0 o la métrica no se registra.	Bytes	• Sum • Media • Mínimo • Máximo

Métrica	Descripción	Unidad	Estadísticas significativas
`MetadataNoToken`	El número de veces que se ha accedido correctamente al servicio de metadatos de instancias (IMDS) mediante un método en el que no se utiliza un token. Esta métrica se utiliza para determinar si hay procesos que acceden a metadatos de la instancia que utiliza el servicio de metadatos de instancias, versión 1 (IMDSv1), que no utilizan un token. Si todas las solicitudes utilizan sesiones basadas en token, por ejemplo, el servicio de metadatos de instancias, versión 2 (IMDSv2), el valor es 0. Para obtener más información, consulte Transición al uso de Servicio de metadatos de instancia, versión 2.	Recuento	• Sum • Percentiles
`MetadataNoTokenRejected`	El número de veces que se intentó hacer una llamada a IMDSv1 después de inhabilitar IMDSv1. Si aparece esta métrica, indica que se intentó llamar a IMDSv1 y se rechazó. Puede volver a activar IMDSv1 o asegurarse de que todas las llamadas utilicen IMDSv2. Para obtener más información, consulte Transición al uso de Servicio de metadatos de instancia, versión 2.	Recuento	• Sum • Percentiles

Métrica	Descripción	Unidad	Estadísticas significativas
`NetworkIn`	El número de bytes recibidos por la instancia en todas las interfaces de red. Esta métrica identifica el volumen de tráfico de red entrante para una sola instancia. El número registrado es el número de bytes recibidos durante el periodo. Si utiliza el monitoreo básico (5 minutos) y la estadísti ca es Suma, puede dividir este número por 300 para conocer los bytes por segundo. Si utiliza el monitoreo detallado (1 minuto) y la estadística es Suma, divídalo por 60. También puede usar la función matemátic a métrica `DIFF_TIME` de CloudWatch para encontrar los bytes por segundo. Por ejemplo, si ha graficado `NetworkIn` en CloudWatch como `m1`, la fórmula matemátic a de métrica `m1/(DIFF_TIME(m1))` devuelve la métrica en bytes/segundo. Para obtener más información sobre `DIFF_TIME` y otras funciones matemáticas de métricas, consulte Uso de matemáticas de métricas en la Guía del usuario de Amazon CloudWatch.	Bytes	• Sum • Media • Mínimo • Máximo

Métrica	Descripción	Unidad	Estadísticas significativas
`NetworkOut`	El número de bytes enviados por la instancia en todas las interfaces de red. Esta métrica identifica el volumen de tráfico de red saliente de una sola instancia. El número registrado es el número de bytes enviados durante el periodo. Si utiliza el monitoreo básico (5 minutos) y la estadística es Suma, puede dividir este número por 300 para conocer los bytes por segundo. Si utiliza el monitoreo detallado (1 minuto) y la estadística es Suma, divídalo por 60. También puede usar la función matemática métrica `DIFF_TIME` de CloudWatch para encontrar los bytes por segundo. Por ejemplo, si ha graficado `NetworkOut` en CloudWatch como `m1`, la fórmula matemática de métrica `m1/(DIFF_TIME(m1))` devuelve la métrica en bytes/segundo. Para obtener más información sobre `DIFF_TIME` y otras funciones matemáticas de métricas, consulte Uso de matemáticas de métricas en la Guía del usuario de Amazon CloudWatch.	Bytes	• Sum • Media • Mínimo • Máximo

Métrica	Descripción	Unidad	Estadísticas significativas
`NetworkPackets In`	El número de paquetes recibidos por la instancia en todas las interfaces de red. Esta métrica identifica el volumen de tráfico de red entrante en cuanto al número de paquetes de una sola instancia. Esta métrica solo se encuentra disponible para el monitoreo básico (periodos de 5 minutos). Para calcular el número de paquetes por segundo (PPS) que recibió la instancia en los 5 minutos, divida el valor de la estadísti ca Suma por 300. También puede usar la función matemática métrica `DIFF_TIME` de CloudWatch para encontrar los paquetes por segundo. Por ejemplo, si ha graficado `NetworkPacketsIn` en CloudWatc h como `m1`, la fórmula matemática métrica `m1/ (DIFF_TIME(m1))` devuelve la métrica en paquetes/segundo. Para obtener más informaci ón sobre `DIFF_TIME` y otras funciones matemáticas de métricas, consulte Uso de matemáticas de métricas en la Guía del usuario de Amazon CloudWatch.	Recuento	• Sum • Media • Mínimo • Máximo

Métrica	Descripción	Unidad	Estadísticas significativas
`NetworkPackets0ut`	El número de paquetes enviados por la instancia en todas las interfaces de red. Esta métrica identifica el volumen de tráfico de red saliente en cuanto al número de paquetes de una sola instancia. Esta métrica solo se encuentra disponible para el monitoreo básico (periodos de 5 minutos). Para calcular el número de paquetes por segundo (PPS) que envió la instancia en los 5 minutos, divida el valor de la estadísti ca Suma por 300. También puede usar la función matemática métrica `DIFF_TIME` de CloudWatch para encontrar los paquetes por segundo. Por ejemplo, si ha graficado `NetworkPackets0ut` en CloudWatch como `m1`, la fórmula matemática métrica `m1/(DIFF_TIME(m1))` devuelve la métrica en paquetes/segundo. Para obtener más información sobre `DIFF_TIME` y otras funciones matemáticas de métricas, consulte Uso de matemáticas de métricas en la Guía del usuario de Amazon CloudWatch.	Recuento	• Sum • Media • Mínimo • Máximo

Métricas de créditos de CPU

El espacio de nombres `AWS/EC2` incluye las siguientes métricas de créditos de CPU para las instancias de rendimiento ampliable.

Métrica	Descripción	Unidad	Estadísticas significativas
`CPUCreditUsage`	La cantidad de créditos de CPU gastados por la instancia para la utilización de la CPU. Un crédito de CPU equivale a una CPU virtual que se ejecuta al 100 % de utilización durante un minuto o una combinación equivalente de unidades de CPU virtuales, utilización y tiempo (por ejemplo, una CPU virtual que se ejecuta al 50 % durante dos minutos o dos CPU virtuales que se ejecutan al 25 % durante dos minutos). Las métricas de créditos de CPU solo se encuentran disponibles cada 5 minutos. Si especifica un periodo superior a cinco minutos, utilice la estadística `Sum` en lugar de `Average`.	Créditos (vCPU/minutos)	• Sum • Media • Mínimo • Máximo
`CPUCreditBalance`	La cantidad de créditos de la CPU obtenidos que una instancia ha acumulado desde que se lanzó o se inició. Para T2 Standard, el `CPUCreditBalance` incluye además el número de créditos de inicialización que se han acumulado. Los créditos se acumulan en el saldo de créditos una vez obtenidos y se eliminan del saldo de créditos cuando se gastan. El saldo de créditos tiene un límite máximo, determinado por el tamaño de la instancia. Una vez que se ha alcanzado el límite, los nuevos créditos obtenidos se descartarán. Para T2 Standard, los créditos de inicialización no cuentan para el límite. Los créditos de `CPUCreditBalance` están disponibles para que la instancia los gaste a	Créditos (vCPU/minutos)	• Sum • Media • Mínimo • Máximo

Métrica	Descripción	Unidad	Estadísticas significativas
	fin de aumentar la utilización de la CPU por encima de la referencia. Cuando una instancia está en ejecución, los créditos en el `CPUCreditBalance` no caducan. Cuando se detiene una instancia T3 o T3a, el valor `CPUCreditBalance` se mantiene durante siete días. A partir de ese momento, se pierden todos los créditos acumulados. Cuando se detiene una instancia T2, el valor de `CPUCreditBalance` no se mantiene y se pierden todos los créditos acumulados. Las métricas de créditos de CPU solo se encuentran disponibles cada 5 minutos.		
`CPUSurplusCreditBalance`	La cantidad de créditos sobrantes que ha gastado una instancia `unlimited` cuando su valor `CPUCreditBalance` es igual a cero. El valor de `CPUSurplusCreditBalance` se compensa con los créditos de CPU obtenidos. Si el número de créditos sobrantes supera el número máximo de créditos que la instancia puede ganar en un periodo de 24 horas, los créditos sobrantes gastados por encima del máximo implican un cargo adicional . Las métricas de créditos de CPU solo se encuentran disponibles cada 5 minutos.	Créditos (vCPU/minutos)	• Sum • Media • Mínimo • Máximo

Métrica	Descripción	Unidad	Estadísticas significativas
`CPUSurplusCreditsCharged`	La cantidad de créditos sobrantes gastados que no se han compensado con créditos de CPU obtenido y, por lo tanto, implican un cargo adicional. Los créditos sobrantes gastados se cobran cuando se da alguno de los casos siguientes: • Los créditos sobrantes gastados superan el número máximo de créditos que la instancia puede obtener en un periodo de 24 horas. Los créditos sobrantes gastados por encima de la cantidad máxima se cobran al final de la hora. • La instancia se detiene o se termina. • La instancia se cambia de `unlimited` a `standard`. Las métricas de créditos de CPU solo se encuentran disponibles cada 5 minutos.	Créditos (vCPU/minutos)	• Sum • Media • Mínimo • Máximo

Métricas de host dedicado

El espacio de nombres `AWS/EC2` incluye las siguientes métricas para host dedicados de T3.

Métrica	Descripción	Unidad	Estadísticas significativas
`DedicatedHostCPUUtilization`	Porcentaje de capacidad informática asignada que están utilizando actualmente las instancias que se ejecutan en el host dedicado.	Porcentaje	• Sum • Media • Mínimo • Máximo

Métricas de Amazon EBS para instancias basadas en Nitro

El espacio de nombres de `AWS/EC2` incluye métricas adicionales de Amazon EBS para los volúmenes que se han adjuntado a instancias basadas en Nitro que no son instancias bare metal.

Métrica	Descripción	Unidad	Estadísticas significativas
`EBSReadOps`	Operaciones de lectura completadas de todos los volúmenes de Amazon EBS conectados a la instancia en un periodo especificado. Para calcular el promedio de operaciones de E/S de lectura por segundo (IOPS de lectura) del periodo, divida el total de operaciones del periodo por el número de segundos de ese periodo. Si utiliza el monitoreo básico (5 minutos), puede dividir este número por 300 para calcular la IOPS de lectura. Si utiliza el monitoreo detallado (1 minuto), divídalo por 60. También puede usar la función matemátic a métrica `DIFF_TIME` de CloudWatch para encontrar las operaciones por segundo. Por ejemplo, si ha graficado `EBSReadOps` en CloudWatch como `m1`, la fórmula matemátic a de métrica `m1/(DIFF_TIME(m1))` devuelve la métrica en operaciones/ segundo. Para obtener más informaci ón sobre `DIFF_TIME` y otras funciones matemáticas de métricas, consulte Uso de matemáticas de métricas en la Guía del usuario de Amazon CloudWatch.	Recuento	• Sum • Media • Mínimo • Máximo
`EBSWriteOps`	Operaciones de escritura completadas en todos los volúmenes de EBS conectados a la instancia en un periodo especificado.	Recuento	• Sum • Media • Mínimo • Máximo

Métrica	Descripción	Unidad	Estadísticas significativas
	Para calcular el promedio de operaciones de E/S de escritura por segundo (IOPS de escritura) del periodo, divida el total de operaciones del periodo por el número de segundos de ese periodo. Si utiliza el monitoreo básico (5 minutos), puede dividir este número por 300 para calcular la IOPS de escritura. Si utiliza el monitoreo detallado (1 minuto), divídalo por 60. También puede usar la función matemática métrica `DIFF_TIME` de CloudWatch para encontrar las operaciones por segundo. Por ejemplo, si ha graficado `EBSWriteOps` en CloudWatch como `m1`, la fórmula matemática de métrica `m1/(DIFF_TIME(m1))` devuelve la métrica en operaciones/segundo. Para obtener más información sobre `DIFF_TIME` y otras funciones matemáticas de métricas, consulte Uso de matemáticas de métricas en la Guía del usuario de Amazon CloudWatch.		

Métrica	Descripción	Unidad	Estadísticas significativas
`EBSReadBytes`	Bytes leídos de todos los volúmenes de EBS conectados a la instancia en un periodo especificado. El número registrado es el número de bytes leídos durante el periodo. Si utiliza el monitoreo básico (5 minutos), puede dividir este número por 300 para conocer los bytes de lectura por segundo. Si utiliza el monitoreo detallado (1 minuto), divídalo por 60. También puede usar la función matemática métrica `DIFF_TIME` de CloudWatch para encontrar los bytes por segundo. Por ejemplo, si ha graficado `EBSReadBytes` en CloudWatch como `m1`, la fórmula matemática de métrica `m1/(DIFF_TIME(m1))` devuelve la métrica en bytes/segundo. Para obtener más información sobre `DIFF_TIME` y otras funciones matemáticas de métricas, consulte Uso de matemáticas de métricas en la Guía del usuario de Amazon CloudWatch.	Bytes	• Sum • Media • Mínimo • Máximo

Métrica	Descripción	Unidad	Estadísticas significativas
`EBSWriteBytes`	Bytes escritos en todos los volúmenes de EBS conectados a la instancia en un periodo especificado. El número registrado es el número de bytes escritos durante el periodo. Si utiliza el monitoreo básico (5 minutos), puede dividir este número por 300 para conocer los bytes de escritura por segundo. Si utiliza el monitoreo detallado (1 minuto), divídalo por 60. También puede usar la función matemática métrica `DIFF_TIME` de CloudWatch para encontrar los bytes por segundo. Por ejemplo, si ha graficado `EBSWriteBytes` en CloudWatch como `m1`, la fórmula matemática de métrica `m1/(DIFF_TIME(m1))` devuelve la métrica en bytes/segundo. Para obtener más información sobre `DIFF_TIME` y otras funciones matemáticas de métricas, consulte Uso de matemáticas de métricas en la Guía del usuario de Amazon CloudWatch.	Bytes	• Sum • Media • Mínimo • Máximo

Métrica	Descripción	Unidad	Estadísticas significativas
`EBSIOBalance%`	Proporciona información sobre el porcentaje de créditos restantes de E/S en el bucket por ráfaga. Esta métrica solo está disponible para la monitorización básica. Esta métrica solo está disponible para algunos tamaños de instancia `*.4xlarge` y otros más pequeños que alcancen su rendimiento máximo durante solo 30 minutos al menos una vez cada 24 horas. La estadística `Sum` no es aplicable a esta métrica.	Porcentaje	• Mínimo • Máximo
`EBSByteBalance%`	Proporciona información sobre el porcentaje de créditos restantes de desempeño en el bucket por ráfaga. Esta métrica solo está disponible para la monitorización básica. Esta métrica solo está disponible para algunos tamaños de instancia `*.4xlarge` y otros más pequeños que alcancen su rendimiento máximo durante solo 30 minutos al menos una vez cada 24 horas. La estadística `Sum` no es aplicable a esta métrica.	Porcentaje	• Mínimo • Máximo

Para obtener más información acerca de las métricas proporcionadas para los volúmenes de EBS, consulte Métricas para los volúmenes de Amazon EBS en la Guía del usuario de Amazon EBS. Para obtener más información acerca de las métricas proporcionadas para las colecciones de spot, consulte Métricas de CloudWatch para las flotas de spot.

Métricas de comprobación de estado

De forma predeterminada, las métricas de comprobación de estado están disponibles con una frecuencia de 1 minuto sin ningún costo adicional. En el caso de una instancia recién lanzada, los datos de las métricas de comprobación de estado solo están disponibles una vez que la instancia ha completado el estado de inicialización (unos minutos después de que la instancia haya entrado en el estado `running`). Para obtener más información acerca de las comprobaciones de estado de EC2, consulte Comprobaciones de estado para sus instancias.

El espacio de nombres `AWS/EC2` incluye las siguientes métricas de comprobaciones de estado.

Métrica	Descripción	Unidad	Estadísticas significativas
`StatusCheckFailed`	Indica si la instancia ha superado la comprobación de estado de la instancia y la comprobación de estado del sistema en el último minuto. Esta métrica puede ser `0` (superada) o `1` (no superada). De forma predeterminada, esta métrica está disponible con una frecuencia de 1 minuto sin ningún costo adicional.	Recuento	• Sum • Media
`StatusCheckFailed_Instance`	Indica si la instancia ha superado la comprobación de estado de la instancia en el último minuto. Esta métrica puede ser `0` (superada) o `1` (no superada). De forma predeterminada, esta métrica está disponible con una frecuencia de 1 minuto sin ningún costo adicional.	Recuento	• Sum • Media
`StatusCheckFailed_System`	Indica si la instancia ha superado la comprobación de estado del sistema en el último minuto.	Recuento	• Sum • Media

Métrica	Descripción	Unidad	Estadísticas significativas
	Esta métrica puede ser `0` (superada) o 1 (no superada). De forma predeterminada, esta métrica está disponible con una frecuencia de 1 minuto sin ningún costo adicional.		
`StatusCheckFailed_AttachedEBS`	Indica si la instancia ha superado la comprobación de estado de EBS adjunta en el último minuto. Esta métrica puede ser `0` (superada) o 1 (no superada). De forma predeterminada, esta métrica está disponible con una frecuencia de 1 minuto sin ningún costo adicional.	Recuento	• Sum • Media

El espacio de nombres `AWS/EBS` incluye la siguiente métrica de comprobaciones de estado.

Métrica	Descripción	Unidad	Estadísticas significativas
`VolumeStalledIOCheck`	Nota: Solo para instancias Nitro. No se publica para los volúmenes adjuntos a Amazon ECS y las tareas de AWS Fargate. Indica si un volumen ha superado o no una comprobación de E/S estancada en el último minuto. Esta métrica puede ser `0` (superada) o 1 (no superada).	Recuento	• Sum • Media • Mínimo • Máximo

Métricas de reflejo de tráfico

El espacio de nombres `AWS/EC2` incluye métricas para el tráfico reflejado. Para obtener más información, consulte Supervisión del tráfico reflejado mediante Amazon CloudWatch en la Guía de reflejo de tráfico de Amazon VPC.

Métricas de grupo de Auto Scaling

El espacio de nombres de `AWS/AutoScaling` incluye métricas para grupos de escalado automático. Para obtener más información, consulte Monitor CloudWatch metrics for your Auto Scaling groups and instances (Supervisión de las métricas de CloudWatch para las instancias y los grupos de escalado automático) en la Guía del usuario de Amazon EC2 Auto Scaling.

Dimensiones de métricas de Amazon EC2

Puede utilizar las siguientes dimensiones para ajustar las métricas mostradas en las tablas anteriores.

Dimensión	Descripción
`AutoScalingGroupName`	Esta dimensión filtra los datos solicitados de todas las instancias en un grupo de capacidad especificado. Un grupo de Auto Scaling es una colección de instancias que usted define si usa Auto Scaling. Esta dimensión solo está disponible para las métricas de Amazon EC2 cuando las instancias están en un grupo de Auto Scaling. Disponible para instancias con la monitorización detallada o básica habilitada.
`ImageId`	Esta dimensión filtra los datos solicitados de todas las instancias que se ejecutan en esta Imagen de máquina de Amazon (AMI) de Amazon EC2. Disponible para instancias con la monitorización detallada habilitada.
`InstanceId`	Esta dimensión filtra únicamente los datos solicitados para la instancia identificada. Sirve para identificar una instancia exacta en la que desee monitorizar datos.
`InstanceType`	Esta dimensión filtra los datos solicitados de todas las instancias que se ejecutan con el tipo de instancia especificado. Esto le

Dimensión	Descripción
	ayuda a clasificar los datos por el tipo de instancia en ejecución . Por ejemplo, puede comparar los datos de una instancia m1.small y una instancia m1.large para determinar cuál de ellas tiene mayor valor empresarial para su aplicación. Disponible para instancias con la monitorización detallada habilitada.

Métricas de uso de Amazon EC2

Puede utilizar las métricas de uso de CloudWatch para proporcionar visibilidad sobre el uso de los recursos de su cuenta. Utilice estas métricas para visualizar el uso actual del servicio en paneles y gráficos de CloudWatch.

Las métricas de uso de Amazon EC2 se corresponden con las cuotas de servicio de AWS. Puede configurar alarmas que le avisen cuando su uso se acerque a una cuota de servicio. Para obtener más información sobre la integración de CloudWatch con Service Quotas, consulte Métricas de uso de AWS en la Guía del usuario de Amazon CloudWatch.

Amazon EC2 publica las siguientes métricas en el espacio de nombres `AWS/Usage`.

Métrica	Descripción
`ResourceCount`	El número de los recursos especificados que se ejecutan en su cuenta. Los recursos se definen por las dimensiones asociadas a la métrica. La estadística más útil para esta métrica es `MAXIMUM`, que representa el número máximo de recursos utilizados durante el periodo de un minuto.

Las siguientes dimensiones se utilizan para ajustar las métricas de uso publicadas por Amazon EC2.

Dimensión	Descripción
`Service`	El nombre del servicio de AWS que contiene el recurso. Para las métricas de uso de Amazon EC2, el valor de esta dimensión es `EC2`.
`Type`	El tipo de entidad que se registra. Actualmente, el único valor válido para las métricas de uso de Amazon EC2 es `Resource`.
`Resource`	El tipo de recurso que se está ejecutando. Actualmente, el único valor válido para las métricas de uso de Amazon EC2 es `vCPU`, que devuelve información sobre las instancias que se están ejecutando.
`Class`	La clase de recurso del que se realiza el seguimiento. Para las métricas de uso de Amazon EC2 con `vCPU` como valor de la dimensión `Resource`, los valores válidos son `Standard/OnDemand` , `F/OnDemand` , `G/OnDemand` , `Inf/OnDemand` , `P/OnDemand` y `X/OnDemand` . Los valores de esta dimensión definen la primera letra de los tipos de instancia registrados por la métrica. Por ejemplo, `Standard/OnDemand` devuelve información sobre todas las instancias en ejecución con tipos que comienzan por A, C, D, H, I, M, R, T y Z, y `G/OnDemand` devuelve información sobre todas las instancias en ejecución con tipos que comienzan por G.

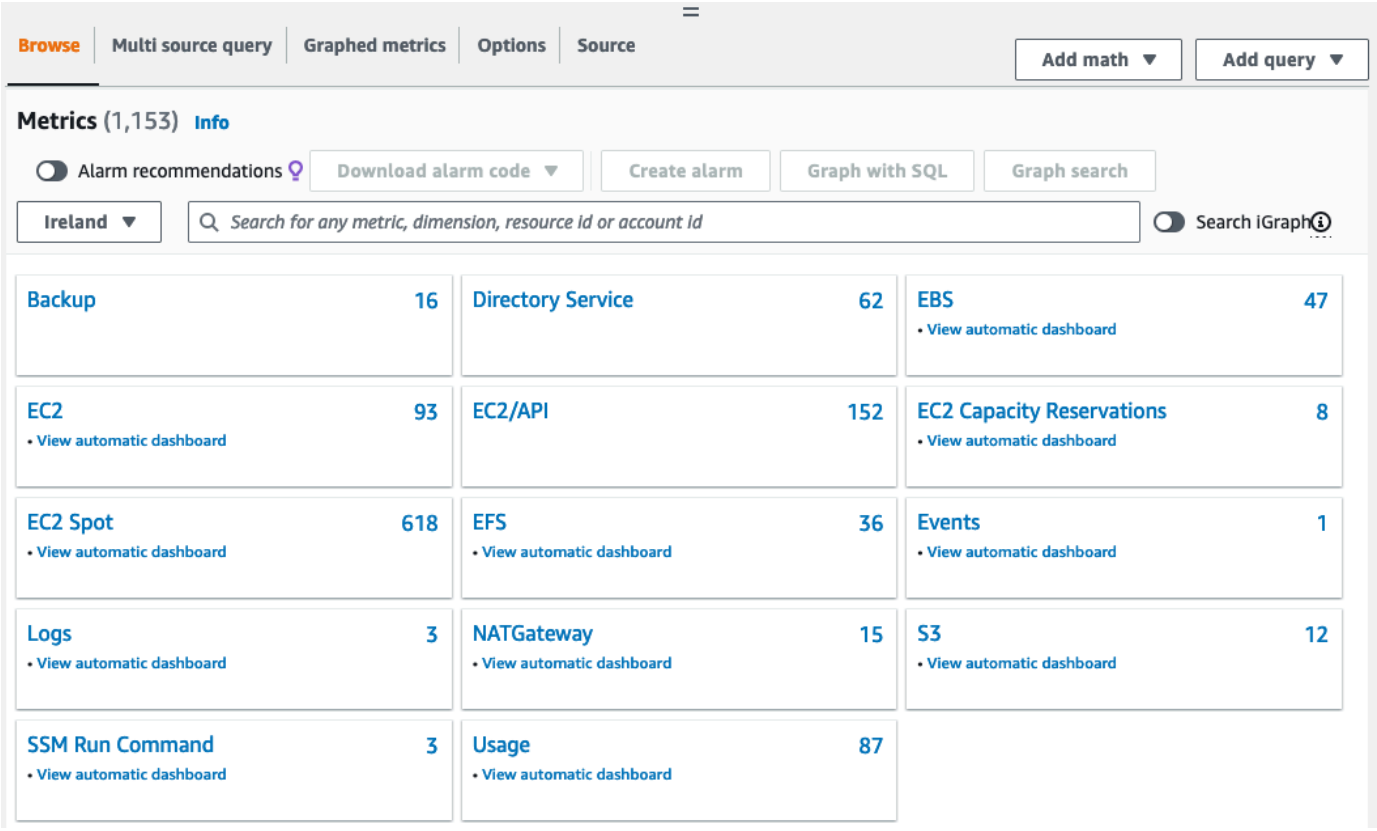
Enumerar las métricas con la consola

Las métricas se agrupan en primer lugar por el espacio de nombres y, a continuación, por las diversas combinaciones de dimensiones dentro de cada espacio de nombres. Por ejemplo, puede ver todas las métricas proporcionadas por Amazon EC2 o las métricas agrupadas por ID de instancia, tipo de instancia, ID de imagen (AMI) o grupo de Auto Scaling.

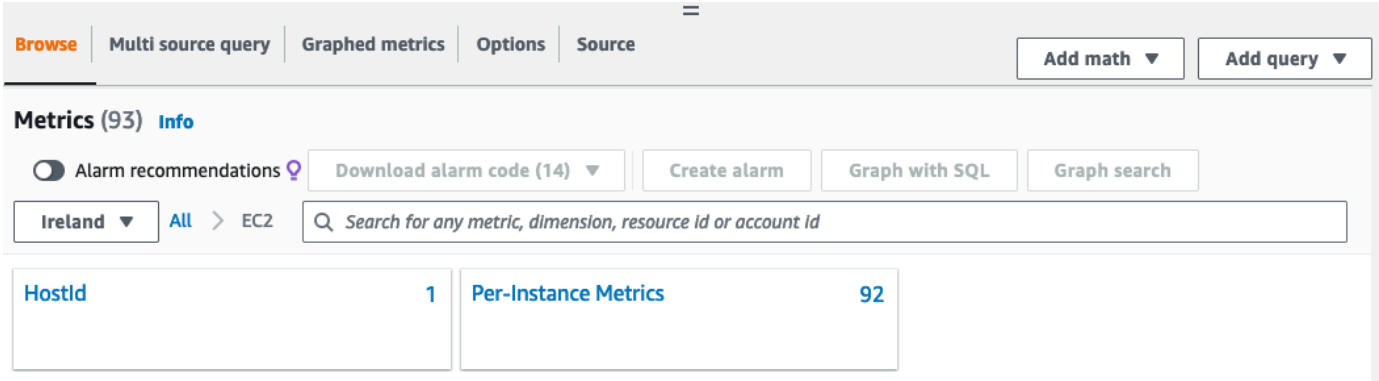
Para ver las métricas disponibles por categoría (consola)

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.

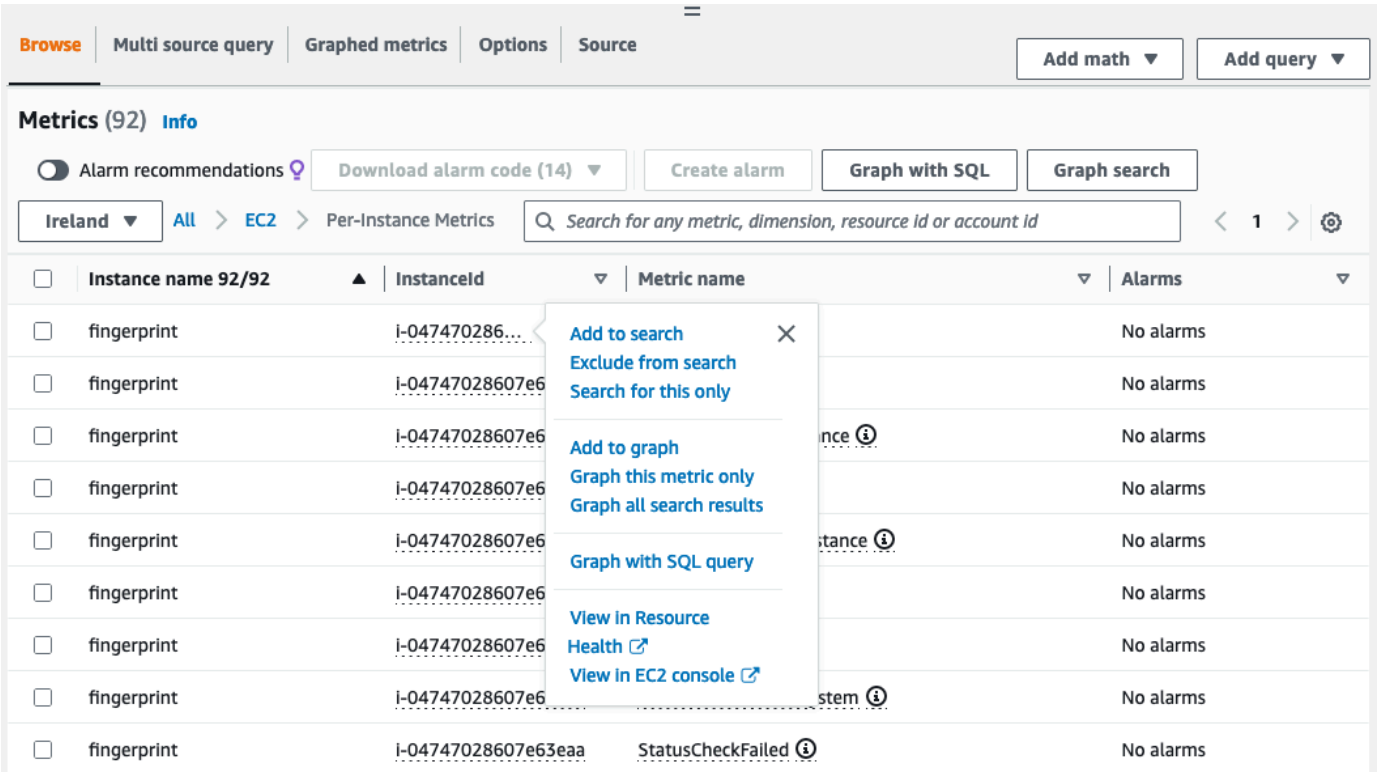
2. En el panel de navegación, expanda Métricas y seleccione Todas las métricas.
3. Elija el espacio de nombres de métrica de EC2.



4. Seleccione una dimensión de métrica (por ejemplo, métricas por instancia).



5. Para ordenar las métricas, utilice el encabezado de columna. Para representar gráficamente una métrica, active la casilla de verificación situada junto a ella. Para filtrar por recurso, seleccione el ID de recurso y, a continuación, elija Add to search (Añadir a la búsqueda). Para filtrar por métrica, elija el nombre de la métrica y, a continuación, seleccione Add to search (Añadir a búsqueda).



Enumerar las métricas con la AWS CLI

Utilice el comando list-metrics para obtener una lista de las métricas de CloudWatch para las instancias.

Para mostrar una lista de todas las métricas disponibles para Amazon EC2 (AWS CLI)

En el siguiente ejemplo, se especifica el espacio de nombres `AWS/EC2` para ver todas las métricas para Amazon EC2.

```
aws cloudwatch list-metrics --namespace AWS/EC2
```

A continuación, se muestra un ejemplo del resultado:

```
{
  "Metrics": [
    {
        "Namespace": "AWS/EC2",
        "Dimensions": [
            {
                "Name": "InstanceId",
                "Value": "i-1234567890abcdef0"
```

```
            }
        ],
        "MetricName": "NetworkOut"
    },
    {
        "Namespace": "AWS/EC2",
        "Dimensions": [
            {
                "Name": "InstanceId",
                "Value": "i-1234567890abcdef0"
            }
        ],
        "MetricName": "CPUUtilization"
    },
    {
        "Namespace": "AWS/EC2",
        "Dimensions": [
            {
                "Name": "InstanceId",
                "Value": "i-1234567890abcdef0"
            }
        ],
        "MetricName": "NetworkIn"
    },
    ...
  ]
}
```

Para mostrar una lista de todas las métricas disponibles para una instancia (AWS CLI)

En el siguiente ejemplo, se especifica el espacio de nombres `AWS/EC2` y la dimensión `InstanceId` para ver los resultados únicamente de la instancia especificada.

```
aws cloudwatch list-metrics --namespace AWS/EC2 --dimensions
 Name=InstanceId,Value=i-1234567890abcdef0
```

Para mostrar una lista de métricas de todas las instancias (AWS CLI)

En el siguiente ejemplo, se especifica el espacio de nombres `AWS/EC2` y un nombre de métrica para ver los resultados únicamente de la métrica especificada.

```
aws cloudwatch list-metrics --namespace AWS/EC2 --metric-name CPUUtilization
```

Instalar y configurar el agente de CloudWatch mediante la consola de Amazon EC2.

La instalación y configuración del agente de CloudWatch mediante la consola de Amazon EC2 se encuentran en fase beta para Amazon EC2 y están sujetas a cambios.

De forma predeterminada, Amazon CloudWatch proporciona métricas básicas, como `CPUUtilization` y `NetworkIn`, para monitorizar las instancias de Amazon EC2. Para recopilar métricas adicionales, puede instalar el agente de CloudWatch en las instancias de EC2 y, a continuación, configurar el agente para que emita las métricas seleccionadas. En lugar de instalar y configurar manualmente el agente de CloudWatch en cada instancia de EC2, puede utilizar la consola Amazon EC2 para que lo haga por usted.

En este tema se explica cómo puede utilizar la consola Amazon EC2 para instalar el agente de CloudWatch en las instancias y configurar el agente para que emita las métricas seleccionadas.

Para ver los pasos manuales de este proceso, consulte Instalación del agente de CloudWatch mediante AWS Systems Manager en la Guía del usuario de Amazon CloudWatch. Para obtener más información sobre el agente de Amazon CloudWatch, consulte Recopilación de métricas, registros y seguimientos con el agente de CloudWatch.

Temas

Requisitos previos

Para utilizar Amazon EC2 a fin de instalar y configurar el agente de CloudWatch, debe cumplir los requisitos previos de usuario e instancia que se describen en esta sección.

Requisitos previos del usuario

Para usar esta característica, el usuario o rol de la consola de IAM debe tener los permisos necesarios para usar Amazon EC2 y los siguientes permisos de IAM:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:GetParameter",
                "ssm:PutParameter"
            ],
            "Resource": "arn:aws:ssm:*:*:parameter/EC2-Custom-Metrics-*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand",
                "ssm:ListCommandInvocations",
                "ssm:DescribeInstanceInformation"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetInstanceProfile",
                "iam:SimulatePrincipalPolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

Requisitos previos para las instancias

- Estado de la instancia: `running`
- Sistema operativo admitido: Linux
- Agente AWS Systems Manager (Agente SSM): instalado. Dos notas sobre el agente SSM:
  - El agente SSM está preinstalado en algunas Imágenes de máquina de Amazon (AMI) AWS proporcionadas por terceros de confianza. Para obtener información sobre las AMI compatibles y

las instrucciones para instalar el agente SSM, consulte Imágenes de máquina de Amazon (AMI) con el agente SSM preinstalado en la Guía del usuario de AWS Systems Manager.

- Si tiene problemas con el agente SSM, consulte Solución de problemas con el agente SSM en la Guía del usuario de AWS Systems Manager.

- Permisos de IAM para la instancia: se deben añadir las siguientes políticas administradas de AWS a un rol de IAM que se ajuste a la instancia:
  - AmazonSSMManagedInstanceCore: permite que una instancia utilice Systems Manager para instalar y configurar el agente de CloudWatch.
  - CloudWatchAgentServerPolicy: permite que una instancia utilice el agente de CloudWatch para escribir datos en CloudWatch.

  Para obtener información sobre cómo añadir permisos de IAM a su instancia, consulte Uso de perfiles de instancia en la Guía del usuario de IAM.

Funcionamiento

Antes de poder utilizar la consola Amazon EC2 para instalar y configurar el agente de CloudWatch, debe asegurarse de que su usuario o rol de IAM y las instancias en las que quiere añadir métricas cumplen ciertos requisitos previos. A continuación, puede utilizar la consola Amazon EC2 para instalar y configurar el agente de CloudWatch en las instancias seleccionadas.

En primer lugar, cumpla con los requisitos previos

- Necesita los permisos de IAM necesarios: antes de empezar, asegúrese de que el usuario o rol de la consola tenga los permisos de IAM necesarios para utilizar esta característica.
- Instancias: para utilizar la característica, las instancias de EC2 deben ser instancias de Linux, tener el agente SSM instalado, tener los permisos de IAM necesarios y estar en ejecución.

A continuación, puede utilizar la característica

1. Seleccione sus instancias: en la consola Amazon EC2, seleccione las instancias en las que desea instalar y configurar el agente de CloudWatch. A continuación, inicie el proceso seleccionando Configurar el agente de CloudWatch.
2. Validar el agente SSM: Amazon EC2 comprueba que el agente SSM esté instalado e iniciado en cada instancia. Las instancias que no superen esta comprobación se excluyen del proceso. El agente SSM se utiliza para realizar acciones en la instancia durante este proceso.

3. Validar los permisos de IAM: Amazon EC2 comprueba que cada instancia tenga los permisos de IAM necesarios para este proceso. Las instancias que no superen esta comprobación se excluyen del proceso. Los permisos de IAM permiten al agente de CloudWatch recopilar métricas de la instancia e integrarlas con AWS Systems Manager para usar el agente SSM.
4. Validar el agente de CloudWatch: Amazon EC2 comprueba que el agente de CloudWatch esté instalado y en ejecución en cada instancia. Si alguna instancia no supera esta comprobación, Amazon EC2 le ofrecerá instalar e iniciar el agente de CloudWatch por usted. El agente de CloudWatch recopilará las métricas seleccionadas en cada instancia una vez que se complete este proceso.
5. Seleccione la configuración de métricas: seleccione las métricas que el agente de CloudWatch emitirá desde sus instancias. Una vez seleccionado, Amazon EC2 almacena un archivo de configuración en el almacén de parámetros, donde permanece hasta que se complete el proceso. Amazon EC2 eliminará el archivo de configuración del almacén de parámetros a menos que se interrumpa el proceso. Tenga en cuenta que si no selecciona una métrica, pero la agregó anteriormente a la instancia, se eliminará de la instancia cuando se complete el proceso.
6. Actualizar la configuración del agente de CloudWatch: Amazon EC2 envía la configuración de métricas al agente de CloudWatch. Este es el último paso del proceso. Si tiene éxito, las instancias pueden emitir datos para las métricas seleccionadas y Amazon EC2 eliminará el archivo de configuración del almacén de parámetros.

Costos

Las métricas adicionales que agregue durante este proceso se facturan como métricas personalizadas. Para obtener más información sobre los precios de las métricas de CloudWatch, consulte Precios de Amazon CloudWatch.

Instalación y configuración del agente de CloudWatch

Puede usar la consola de Amazon EC2 para instalar y configurar el agente de CloudWatch y añadir métricas adicionales.

> **Note**
>
> Cada vez que realiza este procedimiento, sobrescribe la configuración del agente de CloudWatch existente. Si no selecciona una métrica que se haya seleccionado anteriormente, se eliminará de la instancia.

Cómo instalar y configurar el agente de CloudWatch mediante la consola de Amazon EC2

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Seleccione las instancias en las que desea instalar y configurar el agente de CloudWatch.
4. Seleccione Acciones, Supervisar y solucionar problemas, Configurar el agente de CloudWatch.

> **Tip**
>
> Esta característica no está disponible en todas las Regiones de AWS. Si Configurar el agente de CloudWatch no está disponible, pruebe con otra región.

5. Para cada paso del proceso, lea el texto de la consola y, a continuación, seleccione Siguiente.
6. Para completar el proceso, en el paso final, seleccione Completar.

Obtener estadísticas para métricas de las instancias

Puede obtener estadísticas para métricas de CloudWatch de las instancias.

Contenido

Información general de las estadísticas

Las estadísticas son agregaciones de datos de métricas correspondientes a periodos especificados. CloudWatch proporciona estadísticas en función de los puntos de datos de métricas proporcionadas por los datos personalizados o por otros servicios de AWS para CloudWatch. Las acumulaciones se realizan utilizando el espacio de nombres, el nombre de métrica, las dimensiones y la unidad de medida de punto de datos, dentro del período de tiempo que especifique. En la siguiente tabla se describen las estadísticas disponibles.

Estadística	Descripción
`Minimum`	El valor más bajo observado durante el período especificado. Puede utilizar este valor para determinar volúmenes de actividad bajos para su aplicación.
`Maximum`	El valor más alto observado durante el período especificado. Puede utilizar este valor para determinar volúmenes de actividad altos para su aplicación.
`Sum`	Todos los valores enviados para métrica coincidente se suman. Esta estadística puede resultar útil para determinar el volumen total de una métrica.
`Average`	El valor de `Sum`/`SampleCount` durante el periodo específico. Al comparar esta estadística con `Minimum` y `Maximum`, puede determinar el ámbito completo de una métrica y lo cerca que está el uso promedio a los valores `Minimum` y `Maximum`. Esta comparación le ayuda a saber cuándo aumentar o reducir los recursos en función de las necesidades.
`SampleCount`	El recuento (número) de puntos de datos utilizado para el cálculo estadístico.
`pNN.NN`	El valor del percentil especificado. Puede especificar cualquier percentil con hasta dos decimales (por ejemplo, p95.45).

Obtener estadísticas para una instancia específica

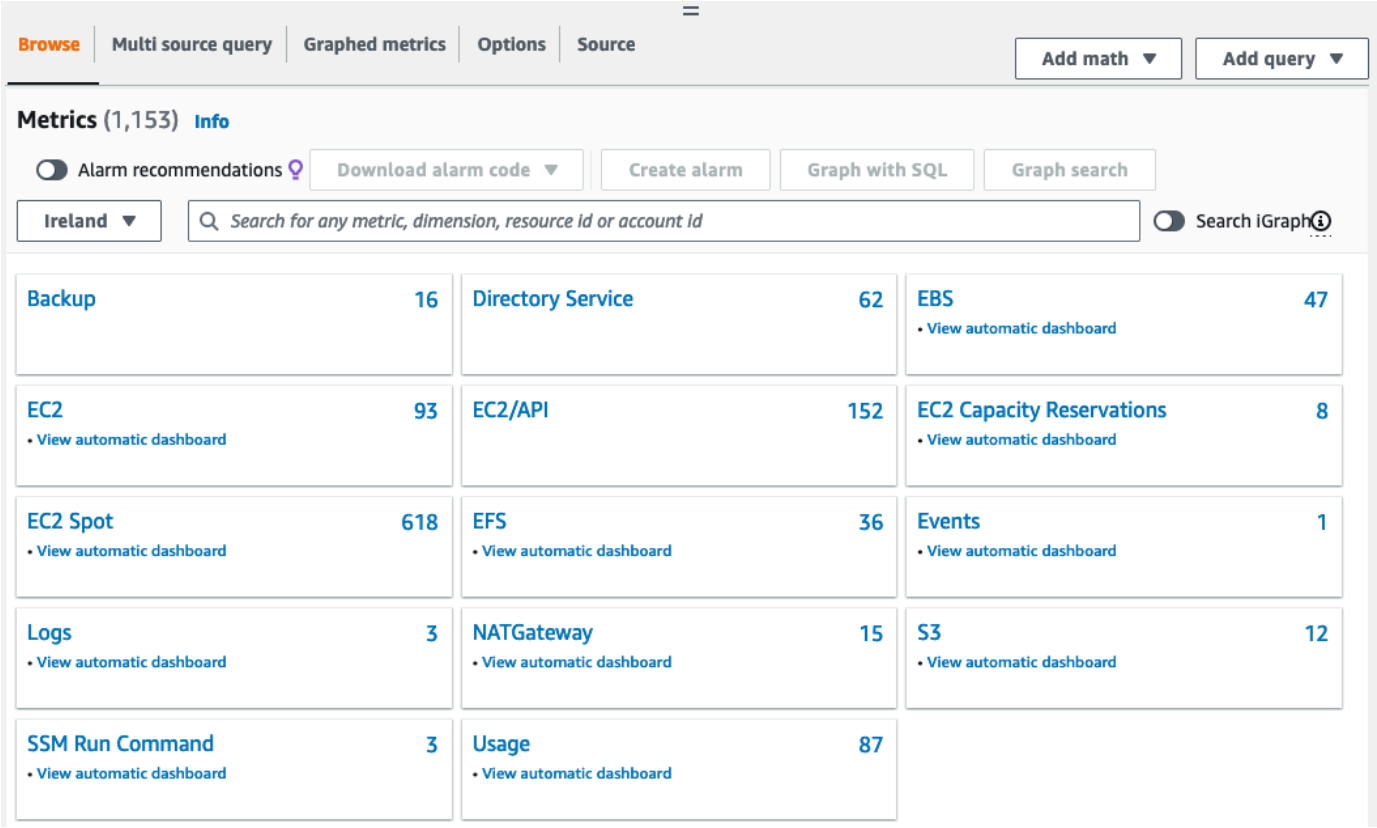
En los siguientes ejemplos se muestra cómo utilizar la AWS Management Console o la AWS CLI para determinar la utilización de CPU máxima de una instancia de EC2 específica.

Requisitos

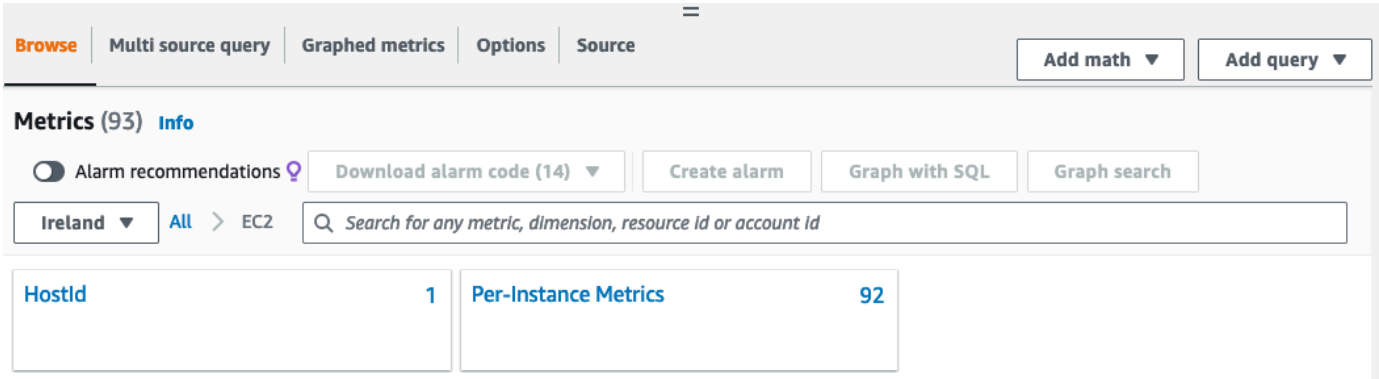
- Debe tener el ID de la instancia. Puede obtener el ID de la instancia mediante la AWS Management Console o el comando describe-instances.
- De forma predeterminada, la monitorización básica está habilitada, pero puede activar la monitorización detallada. Para obtener más información, consulte Activar o desactivar el monitoreo detallado para las instancias.

Para mostrar la utilización de la CPU de una instancia concreta (consola)

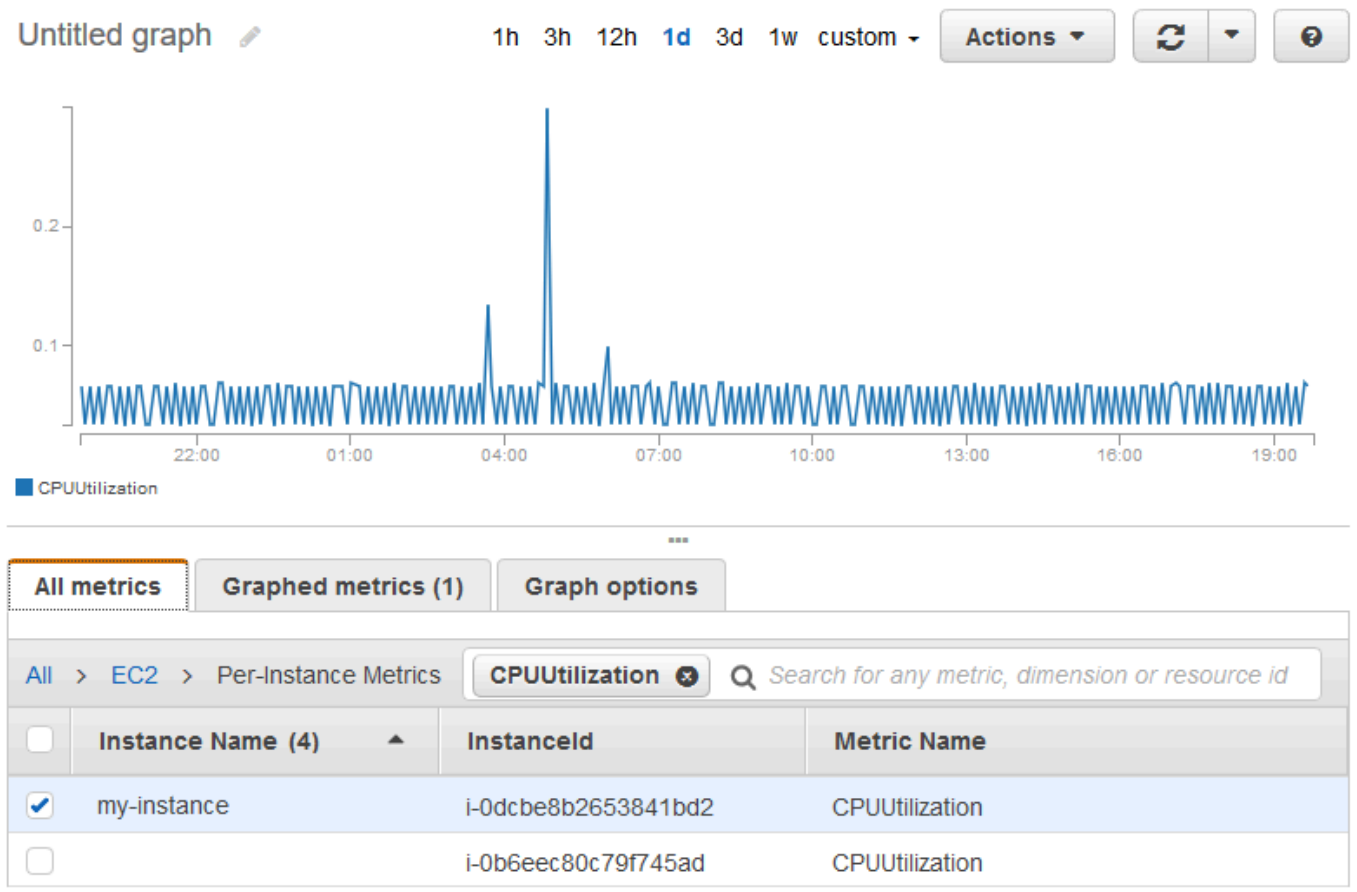
1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, elija Metrics (Métricas).
3. Elija el espacio de nombres de métrica de EC2.



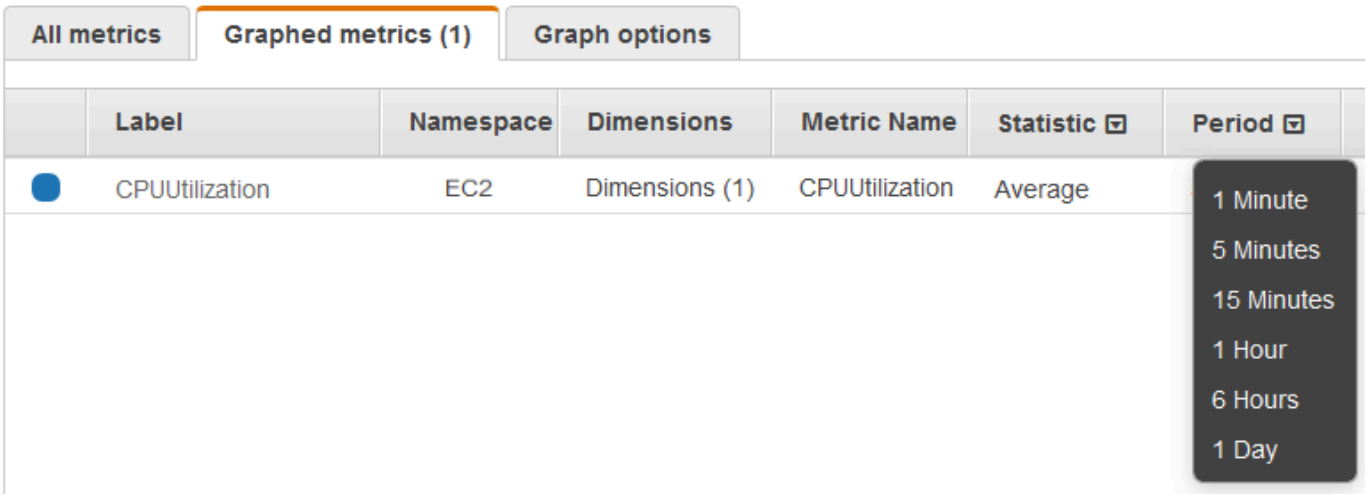
4. Elija la dimensión Per-Instance Metrics (Métricas por instancia).



5. En el campo de búsqueda, escriba **`CPUUtilization`** y pulse Intro. Elija la fila de la instancia concreta, que muestra un gráfico para la métrica CPUUtilization de la instancia. Para asignar un nombre al gráfico, elija el icono del lápiz. Para cambiar el intervalo de tiempo, seleccione uno de los valores predefinidos o elija custom (personalizado).



6. Para cambiar la estadística o el periodo de la métrica, elija la pestaña Graphed metrics (Métricas diagramadas). Elija el encabezado de columna o un valor individual y, a continuación, elija un valor diferente.



Para obtener la utilización de la CPU de una instancia concreta (AWS CLI)

Utilice el siguiente comando get-metric-statistics para obtener la métrica CPUUtilization para la instancia especificada utilizando el periodo y el intervalo de tiempo especificados:

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name CPUUtilization
 --period 3600 \
--statistics Maximum --dimensions Name=InstanceId,Value=i-1234567890abcdef0 \
--start-time 2022-10-18T23:18:00 --end-time 2022-10-19T23:18:00
```

A continuación, se muestra un ejemplo del resultado. Cada valor representa el porcentaje de utilización de CPU máxima para una sola instancia de EC2.

```
{
    "Datapoints": [
        {
            "Timestamp": "2022-10-19T00:18:00Z",
            "Maximum": 0.33000000000000002,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-19T03:18:00Z",
            "Maximum": 99.670000000000002,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-19T07:18:00Z",
            "Maximum": 0.34000000000000002,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-19T12:18:00Z",
            "Maximum": 0.34000000000000002,
            "Unit": "Percent"
        },
        ...
    ],
    "Label": "CPUUtilization"
}
```

Acumular estadísticas para distintas instancias

Las estadísticas agrupadas están disponibles para las instancias que tengan el monitoreo detallado habilitado. Las instancias que utilizan la monitorización básica no están incluidas en las estadísticas

acumulas. Antes de poder obtener estadísticas agrupadas en todas las instancias, debe habilitar el monitoreo detallado (con un cargo adicional), que proporciona datos en periodos de 1 minuto.

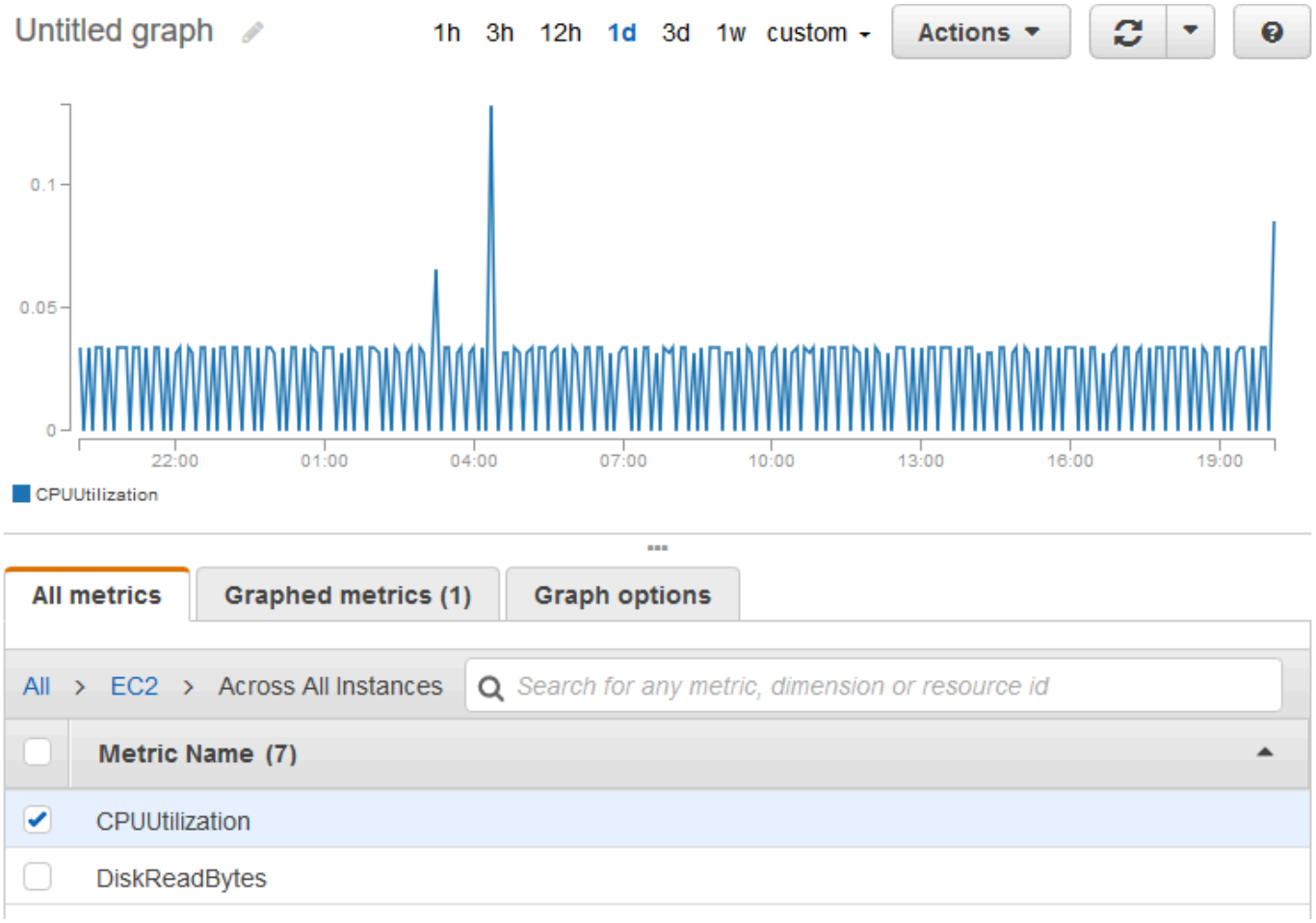
Tenga en cuenta que Amazon CloudWatch no puede agrupar datos en las regiones de AWS. Las métricas son totalmente independientes entre regiones.

Este ejemplo muestra cómo utilizar la monitorización detallada para obtener el uso promedio de CPU de las instancias de EC2. Dado que no se especifica ninguna dimensión, CloudWatch devuelve estadísticas para todas las dimensiones en el espacio de nombres `AWS/EC2`.

> **Important**
>
> Esta técnica que se utiliza en la recuperación de todas las dimensiones en un espacio de nombres de AWS no funciona para espacios de nombres personalizados que publique en Amazon CloudWatch. Con el uso de espacios de nombres personalizados, debe especificar el conjunto completo de dimensiones que hay asociadas a cualquier punto de datos dado para recuperar estadísticas que incluyen el punto de datos.

Para mostrar la utilización media de la CPU en sus instancias (consola)

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, seleccione Metrics (Métricas).
3. Elija el espacio de nombres EC2 y seleccione Across All Instances (En todas las instancias).
4. Elija la fila que contiene CPUUtilization, que muestra un gráfico de la métrica de todas sus instancias de EC2. Para asignar un nombre al gráfico, elija el icono del lápiz. Para cambiar el intervalo de tiempo, seleccione uno de los valores predefinidos o elija custom (personalizado).



5. Para cambiar la estadística o el periodo de la métrica, elija la pestaña Graphed metrics (Métricas diagramadas). Elija el encabezado de columna o un valor individual y, a continuación, elija un valor diferente.

Para obtener la utilización media de la CPU en sus instancias (AWS CLI)

Utilice el comando get-metric-statistics como se indica a continuación para obtener la métrica del promedio de CPUUtilization para las distintas instancias:

```
aws cloudwatch get-metric-statistics \
    --namespace AWS/EC2 \
    --metric-name CPUUtilization \
    --period 3600  --statistics "Average" "SampleCount" \
    --start-time 2022-10-11T23:18:00 \
    --end-time 2022-10-12T23:18:00
```

A continuación, se muestra un ejemplo del resultado:

```
{
    "Datapoints": [
        {
            "SampleCount": 238.0,
            "Timestamp": "2022-10-12T07:18:00Z",
            "Average": 0.038235294117647062,
            "Unit": "Percent"
        },
        {
            "SampleCount": 240.0,
            "Timestamp": "2022-10-12T09:18:00Z",
            "Average": 0.16670833333333332,
            "Unit": "Percent"
        },
        {
            "SampleCount": 238.0,
            "Timestamp": "2022-10-11T23:18:00Z",
            "Average": 0.041596638655462197,
            "Unit": "Percent"
        },
        ...
    ],
    "Label": "CPUUtilization"
}
```


Acumular estadísticas por grupo de Auto Scaling

Puede acumular estadísticas para las instancias de EC2 en un grupo de Auto Scaling. Tenga en cuenta que Amazon CloudWatch no puede agrupar datos en las regiones de AWS. Las métricas son totalmente independientes entre regiones.

En este ejemplo, se muestra cómo recuperar los bytes totales que se escriben en disco para un grupo de Auto Scaling. El total se calcula para periodos de 1 minuto para un intervalo de 24 horas en todas las instancias de EC2 en el grupo de Auto Scaling especificado.

Para visualizar DiskWriteBytes para las instancias en un grupo de Auto Scaling (consola)

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, seleccione Metrics (Métricas).
3. Elija el espacio de nombres EC2 y, a continuación, seleccione By Auto Scaling Group (Por grupo de Auto Scaling).

4. Elija la fila para la métrica DiskWriteBytes y el grupo de Auto Scaling específico, que muestra un gráfico para la métrica para las instancias en el grupo de Auto Scaling. Para asignar un nombre al gráfico, elija el icono del lápiz. Para cambiar el intervalo de tiempo, seleccione uno de los valores predefinidos o elija custom (personalizado).
5. Para cambiar la estadística o el periodo de la métrica, elija la pestaña Graphed metrics (Métricas diagramadas). Elija el encabezado de columna o un valor individual y, a continuación, elija un valor diferente.

Para visualizar DiskWriteBytes para las instancias en un grupo de Auto Scaling (AWS CLI)

Utilice el comando get-metric-statistics como se indica a continuación.

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name DiskWriteBytes
 --period 360 \
--statistics "Sum" "SampleCount" --dimensions Name=AutoScalingGroupName,Value=my-asg --
start-time 2022-10-16T23:18:00 --end-time 2022-10-18T23:18:00
```

A continuación, se muestra un ejemplo del resultado:

```
{
    "Datapoints": [
        {
            "SampleCount": 18.0,
            "Timestamp": "2022-10-19T21:36:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
        },
        {
            "SampleCount": 5.0,
            "Timestamp": "2022-10-19T21:42:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
        }
    ],
    "Label": "DiskWriteBytes"
}
```

Acumular estadísticas por AMI

Puede acumular estadísticas para las instancias que tengan la monitorización detallada habilitada. Las instancias que utilizan la monitorización básica no están incluidas en las estadísticas acumulas. Antes de poder obtener estadísticas agrupadas en todas las instancias, debe habilitar el monitoreo detallado (con un cargo adicional), que proporciona datos en periodos de 1 minuto.

Tenga en cuenta que Amazon CloudWatch no puede agrupar datos en las regiones de AWS. Las métricas son totalmente independientes entre regiones.

Este ejemplo muestra cómo determinar la utilización promedio de la CPU de todas las instancias que utilizan una Imagen de máquina de Amazon (AMI) específica. La media está por encima de intervalos de tiempo de 60 segundos durante un periodo de un día.

Para mostrar la utilización media de CPU por AMI (consola)

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, seleccione Metrics (Métricas).
3. Elija el espacio de nombres EC2 y, a continuación, seleccione By Image (AMI) Id (Por ID de imagen (AMI)).
4. Elija la fila para la métrica CPUUtilization y la AMI específica, que muestra un gráfico para la métrica para la AMI especificada. Para asignar un nombre al gráfico, elija el icono del lápiz. Para cambiar el intervalo de tiempo, seleccione uno de los valores predefinidos o elija custom (personalizado).
5. Para cambiar la estadística o el periodo de la métrica, elija la pestaña Graphed metrics (Métricas diagramadas). Elija el encabezado de columna o un valor individual y, a continuación, elija un valor diferente.

Para obtener la utilización media de la CPU de un ID de imagen (AWS CLI)

Utilice el comando get-metric-statistics como se indica a continuación.

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name CPUUtilization
 --period 3600 \
--statistics Average --dimensions Name=ImageId,Value=ami-3c47a355 --start-
time 2022-10-10T00:00:00 --end-time 2022-10-11T00:00:00
```

A continuación, se muestra un ejemplo del resultado. Cada valor representa un porcentaje de utilización de CPU promedio para las instancias de EC2 que ejecutan la AMI especificada.

```
{
    "Datapoints": [
        {
            "Timestamp": "2022-10-10T07:00:00Z",
            "Average": 0.041000000000000009,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-10T14:00:00Z",
            "Average": 0.079579831932773085,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-10T06:00:00Z",
            "Average": 0.036000000000000011,
            "Unit": "Percent"
        },
        ...
    ],
    "Label": "CPUUtilization"
}
```

Representación gráfica de métricas para las instancias

Tras lanzar la instancia, puede abrir la consola de Amazon EC2 y ver los gráficos de monitorización de la instancia en la pestaña Monitoring (Monitorización). Cada gráfico se basa en una de las métricas de Amazon EC2 disponibles.

Están disponibles los siguientes gráficos:

- Utilización media de la CPU (porcentaje)
- Número medio de operaciones de lectura en disco (bytes)
- Número medio de operaciones de escritura en disco (bytes)
- Entrada de red máxima (bytes)
- Salida de red máxima (bytes)
- Resumen de operaciones de lectura en disco (recuento)
- Resumen de operaciones de escritura en disco (recuento)

- Resumen de estado (cualquiera)
- Resumen de estado instancia (recuento)
- Resumen de estado sistema (recuento)

Para obtener más información acerca de las métricas y los datos que proporcionan a los gráficos, consulte Mostrar las métricas de CloudWatch disponibles para las instancias.

Representación gráfica de métricas mediante la consola de CloudWatch

También puede utilizar la consola de CloudWatch para representar gráficamente datos de métricas generados por Amazon EC2 y otros servicios de AWS. Para obtener más información, consulte Representación gráfica de métricas en la Guía del usuario de Amazon CloudWatch.

Crear una alarma de CloudWatch para una instancia

Puede crear una alarma de CloudWatch que monitoree métricas de CloudWatch para una de sus instancias. CloudWatch le enviará una notificación automáticamente cuando la métrica alcance un límite que haya especificado. Puede crear una alarma de CloudWatch mediante la consola de Amazon EC2 o bien utilizando las opciones más avanzadas que proporciona la consola de CloudWatch.

Para crear una alarma mediante la consola de CloudWatch

Para ver ejemplos, consulte Creación de alarmas de Amazon CloudWatch en la Guía del usuario de Amazon CloudWatch.

Para crear una alarma mediante la consola de Amazon EC2

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancias).
3. Seleccione la instancia y elija Actions (Acciones), Monitoring and troubleshoot (Monitoreo y solución de problemas), Manage CloudWatch alarms (Administrar alarmas de CloudWatch).
4. En la página de detalles Manage CloudWatch alarms (Administrar alarmas de CloudWatch), en Add or edit alarm (Agregar o editar alarma), seleccione Create an alarm (Crear una alarma).
5. En Notificación de alarma, elija si desea configurar las notificaciones de Amazon Simple Notification Service (Amazon SNS). Introduzca un tema de Amazon SNS existente o escriba un nombre para crear un nuevo tema.

6. En Acción de alarma, elija si desea especificar una acción que se debe llevar a cabo cuando se active la alarma. Elija una acción de la lista.
7. En Alarm thresholds (Umbrales de alarma), seleccione la métrica y los criterios para la alarma. Por ejemplo, para crear una alarma que se active cuando el uso de la CPU alcance el 80 % durante un periodo de 5 minutos, haga lo siguiente:
   a. Deje la configuración predeterminada para Agrupar muestras por (Promedio) y Tipo de datos para la muestra (Utilización de CPU).
   b. Elija >= en Alarma cuando e ingrese **`0.80`** para Porcentaje.
   c. Ingrese **`1`** para Periodo consecutivo y seleccione 5 minutos para Periodo.
8. (Opcional) En Sample metric data (Muestrear datos de métrica), elija Add to dashboard (Agregar al panel).
9. Seleccione Create (Crear).

Puede editar la configuración de la alarma de CloudWatch desde la consola de Amazon EC2 o la consola de CloudWatch. Si desea eliminar la alarma, puede hacerlo desde la consola de CloudWatch. Para obtener más información, consulte Edición o eliminación de una alarma de CloudWatch en Guía del usuario de Amazon CloudWatch.

Crear alarmas que detienen, terminan, reinician o recuperan una instancia

Mediante las acciones de alarma de Amazon CloudWatch, puede crear alarmas que detienen, terminan, reinician o recuperan automáticamente las instancias. Puede utilizar las acciones detener o terminar para ayudarle a ahorrar dinero cuando ya no necesita que se ejecute una instancia. Puede utilizar las acciones reiniciar y recuperar para reiniciar automáticamente dichas instancias o recuperarlas en nuevo hardware si se produce un deterioro del sistema.

> **Note**
>
> Para obtener información sobre facturación y costos de alarmas de Amazon CloudWatch, consulte Facturación y costo de CloudWatch en la Guía del usuario de Amazon CloudWatch.

El rol vinculado a servicio `AWSServiceRoleForCloudWatchEvents` permite a AWS realizar acciones de alarma en su nombre. La primera vez que se crea una alarma en la AWS Management Console, la AWS CLI o la API de IAM, CloudWatch crea el rol vinculado al servicio automáticamente.

Hay una serie de situaciones en las que es posible que desee detener o terminar la instancia automáticamente. Por ejemplo, es posible que tenga instancias dedicadas a trabajos de procesamiento de nóminas por lotes o tareas de cálculo científico que se ejecutan durante un período de tiempo y después completan su trabajo. En lugar de dejar dichas instancias inactivas (y acumulando cargos), puede detenerlas o terminarlas, lo que le permitirá ahorrar dinero. La principal diferencia entre utilizar las acciones de alarma ”detener” y ”terminar” es que una instancia detenida puede reiniciarse fácilmente si es necesario volver a ejecutarla más tarde y puede mantener el mismo ID de instancia y el mismo volumen raíz. Por el contrario, una instancia terminada no se puede reiniciar. En su lugar, debe lanzar una nueva instancia. Los volúmenes de almacén de instancias se perderán cuando se detenga o termine una instancia.

Puede agregar las acciones de detener, terminar, reiniciar o recuperar a cualquier alarma establecida en una métrica por instancia Amazon EC2, incluidas las métricas de monitoreo básicas y detalladas proporcionadas por Amazon CloudWatch (en el espacio de nombres `AWS/EC2`), así como cualquier métrica personalizada que incluya la dimensión `InstanceId`, siempre que su valor se refiera a una instancia de Amazon EC2 válida en ejecución.

> **Important**
>
> Las alarmas de comprobación de estado pueden mostrar temporalmente el estado de `INSUFFICIENT_DATA` si faltan puntos de datos de las métricas. Aunque es poco frecuente, esto puede ocurrir cuando se produce una interrupción en los sistemas de generación de informes de las métricas, incluso cuando una instancia está en buen estado. Le recomendamos que entienda el estado de `INSUFFICIENT_DATA` como un aviso de que faltan datos y no como una interrupción de la alarma, en especial cuando configure la alarma para detener, finalizar, reiniciar o recuperar una instancia.

Soporte de consola

Puede crear alarmas mediante la consola de Amazon EC2 o la consola de CloudWatch. Los procedimientos de esta documentación utilizan la consola de Amazon EC2. Para ver los procedimientos que utilizan la consola de CloudWatch, consulte Crear alarmas que detengan, terminen, reinicien o recuperen una instancia en la Guía del usuario de Amazon CloudWatch.

Permisos

Debe tener el `iam:CreateServiceLinkedRole` para crear o modificar una alarma que realice acciones de la alarma de EC2. Un rol de servicio es un rol de IAM que asume un servicio para

realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

Contenido

Agregar acciones de detención a las alarmas Amazon CloudWatch

Puede crear una alarma que detenga una instancia Amazon EC2 cuando se alcance un umbral determinado. Por ejemplo, podría ejecutar instancias de desarrollo o de prueba y en ocasiones olvidarse de apagarlas. Puede crear una alarma que se active cuando el porcentaje de uso medio de la CPU haya estado por debajo del 10 por ciento durante 24 horas, hecho indicativo de que ha estado inactiva y que ya no se está usando. Puede ajustar el umbral, la duración y el periodo que mejor se adapten a sus necesidades, y además puede añadir una notificación de Amazon Simple Notification Service (Amazon SNS) para recibir un correo electrónico cuando se active la alarma.

Las instancias utilizan un volumen de Amazon EBS como dispositivo raíz se pueden detener o terminar, mientras que aquellas que utilizan el almacén de instancias como dispositivo raíz solo se pueden terminar. Los datos almacenados en volúmenes de almacén de instancias se perderán cuando se termine o detenga la instancia.

Para crear una alarma para parar una instancia inactiva (consola de Amazon EC2)

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancias).
3. Seleccione la instancia y elija Actions (Acciones) (Acciones), Monitoring and troubleshoot (Monitoreo y solución de problemas), Manage CloudWatch alarms (Administrar alarmas de CloudWatch).

Alternativamente, puede elegir el signo más (

) en la columna Alarm status (Estado de alarma).

4. En la página Manage CloudWatch alarms (Administrar alarmas de CloudWatch), realice lo siguiente:

   a. Elija Create an alarm (Crear una alarma).

   b. Para recibir un correo electrónico cuando se activa la alarma, en Alarm notification (Notificación de alarma), elija un tema Amazon SNS existente. Primero debe crear un tema de Amazon SNS mediante la consola de Amazon SNS. Para obtener más información, consulte Uso de Amazon SNS para mensajería de aplicación a persona (A2P) en Guía para desarrolladores de Amazon Simple Notification Service.

   c. Cambie Alarm action (Acción de alarma) y elija Stop (Detener).

   d. En Group samples by (Agrupar muestras por) y Type of data to sample (Tipo de datos para mostrar), elija una estadística y una métrica. En este ejemplo, elija Average (Promedio) y CPU utilization (Utilización de la CPU).

   e. En Alarm When (Alarma cuando) y Percent (Porcentaje), especifique el umbral de métrica. En este ejemplo, especifique <= y 10 por ciento.

   f. En Consecutive period (Periodo consecutivo) y Period (Periodo), especifique el periodo de evaluación de la alarma. En este ejemplo, especifique 1 periodo consecutivo de 5 Minutes (5 minutos).

   g. Amazon CloudWatch crea automáticamente un nombre de alarma para usted. Para cambiar el nombre, en Alarm name (Nombre de alarma), ingrese un nombre nuevo. Los nombres de alarma solo pueden contener caracteres ASCII.

      > **Note**
      >
      > Puede ajustar la configuración de la alarma en función de sus propios requisitos antes de crear la alarma, o puede editarla más adelante. Esto incluye la configuración de la métrica, el umbral, la duración, la acción y la notificación. Sin embargo, después de crear una alarma, no podrá editar su nombre más adelante.

   h. Seleccione Create (Crear).

Agregar acciones de terminación a alarmas de Amazon CloudWatch

Puede crear una alarma que termina una instancia de EC2 automáticamente cuando se alcanza un umbral determinado (siempre y cuando la protección de terminación no esté habilitada para la instancia). Por ejemplo, es posible que desee terminar una instancia cuando haya completado su trabajo y no necesite la instancia de nuevo. En caso de que desee utilizar la instancia en otro momento, debe detener la instancia en lugar de terminarla. Los datos almacenados en volúmenes de almacén de instancias se perderán cuando se. termine la instancia. Para obtener información sobre cómo habilitar y deshabilitar la protección de terminación para una instancia, consulte Cómo habilitar la protección contra la terminación.

Para crear una alarma para terminar una instancia inactiva (consola de Amazon EC2)

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancias).
3. Seleccione la instancia y elija Actions (Acciones) (Acciones), Monitoring and troubleshoot (Monitoreo y solución de problemas), Manage CloudWatch alarms (Administrar alarmas de CloudWatch).

   Alternativamente, puede elegir el signo más (

) en la columna Alarm status (Estado de alarma).
4. En la página Manage CloudWatch alarms (Administrar alarmas de CloudWatch), realice lo siguiente:

   a. Elija Create an alarm (Crear una alarma).

   b. Para recibir un correo electrónico cuando se activa la alarma, en Alarm notification (Notificación de alarma), elija un tema Amazon SNS existente. Primero debe crear un tema de Amazon SNS mediante la consola de Amazon SNS. Para obtener más información, consulte Uso de Amazon SNS para mensajería de aplicación a persona (A2P) en Guía para desarrolladores de Amazon Simple Notification Service.

   c. Cambie Alarm action (Acción de alarma) y elija Terminate (Terminar).

   d. En Group samples by (Agrupar muestras por) y Type of data to sample (Tipo de datos para mostrar), elija una estadística y una métrica. En este ejemplo, elija Average (Promedio) y CPU utilization (Utilización de la CPU).

e. En Alarm When (Alarma cuando) y Percent (Porcentaje), especifique el umbral de métrica. En este ejemplo, especifique >= y 10 por ciento.

f. En Consecutive period (Periodo consecutivo) y Period (Periodo), especifique el periodo de evaluación de la alarma. En este ejemplo, especifique 24 periodos consecutivos de 1 Hour (1 hora).

g. Amazon CloudWatch crea automáticamente un nombre de alarma para usted. Para cambiar el nombre, en Alarm name (Nombre de alarma), ingrese un nombre nuevo. Los nombres de alarma solo pueden contener caracteres ASCII.

> **Note**
>
> Puede ajustar la configuración de la alarma en función de sus propios requisitos antes de crear la alarma, o puede editarla más adelante. Esto incluye la configuración de la métrica, el umbral, la duración, la acción y la notificación. Sin embargo, después de crear una alarma, no podrá editar su nombre más adelante.

h. Seleccione Create (Crear).

Agregar acciones de reinicio a alarmas de Amazon CloudWatch

Puede crear una alarma de Amazon CloudWatch que monitorice una instancia Amazon EC2 y reinicie la instancia automáticamente. La acción de alarma de reinicio se recomienda para errores de comprobación de estado de instancia (en contraposición a la acción de alarma recuperar, que es adecuada para los errores de comprobación de estado del sistema). Un reinicio de instancia es equivalente a un reinicio del sistema operativo. En la mayoría de los casos, solo necesita unos minutos para reiniciar su instancia. Cuando se reinicia una instancia, sigue estando en el mismo host físico, por lo que la instancia mantiene su nombre de DNS público, dirección IP privada y todos los datos en sus volúmenes de almacén de instancia.

Con el reinicio de una instancia, no se comienza un periodo nuevo de facturación de instancia (con un cargo mínimo de un minuto), a diferencia de la detención y la reanudación de la instancia. Los datos almacenados en volúmenes de almacén de instancias se retienen cuando la instancia se reinicia. Los volúmenes de almacén de instancias se deben volver a montar en el sistema de archivos después de un reinicio. Para obtener más información, consulte Reinicio de su instancia.

> **Important**
>
> Para evitar una condición de carrera entre las acciones de reinicio y de recuperación, evite configurar el mismo número de periodos de evaluación para una alarma de reinicio y otra de recuperación. Le recomendamos que configure las alarmas de reinicio en tres periodos de un minuto cada uno. Para obtener más información, consulte Evaluación de una alarma en la Guía del usuario de Amazon CloudWatch.

Para crear una alarma para reiniciar una instancia inactiva (consola de Amazon EC2)

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancias).
3. Seleccione la instancia y elija Actions (Acciones) (Acciones), Monitoring and troubleshoot (Monitoreo y solución de problemas), Manage CloudWatch alarms (Administrar alarmas de CloudWatch).

   Alternativamente, puede elegir el signo más (

) en la columna Alarm status (Estado de alarma).
4. En la página Manage CloudWatch alarms (Administrar alarmas de CloudWatch), realice lo siguiente:

   a. Elija Create an alarm (Crear una alarma).

   b. Para recibir un correo electrónico cuando se activa la alarma, en Alarm notification (Notificación de alarma), elija un tema Amazon SNS existente. Primero debe crear un tema de Amazon SNS mediante la consola de Amazon SNS. Para obtener más información, consulte Uso de Amazon SNS para mensajería de aplicación a persona (A2P) en Guía para desarrolladores de Amazon Simple Notification Service.

   c. Cambie Alarm action (Acción de alarma) y elija Reboot (Reiniciar).

   d. En Group samples by (Agrupar muestras por) y Type of data to sample (Tipo de datos para mostrar), elija una estadística y una métrica. En este ejemplo, elija Average (Promedio) y Status check failed: instance (Comprobación de estado no superada: instancia).

   e. En Consecutive period (Periodo consecutivo) y Period (Periodo), especifique el periodo de evaluación de la alarma. En este ejemplo, escriba 3 periodos consecutivos de 5 Minutes (5 minutos).

f. Amazon CloudWatch crea automáticamente un nombre de alarma para usted. Para cambiar el nombre, en Alarm name (Nombre de alarma), ingrese un nombre nuevo. Los nombres de alarma solo pueden contener caracteres ASCII.

g. Seleccione Create (Crear).

Agregar acciones de recuperación a alarmas de Amazon CloudWatch

Puede crear una alarma de Amazon CloudWatch que monitorice una instancia Amazon EC2. Si la instancia deja de funcionar debido a un error de hardware subyacente o a un problema que requiera la implicación de AWS para la reparación, puede recuperar automáticamente la instancia. Las instancias terminadas no se pueden recuperar. Una instancia recuperada es idéntica a la instancia original, incluido el ID de instancia, direcciones IP privadas, direcciones IP elásticas y todos los metadatos de la instancia.

CloudWatch le impide añadir una acción de recuperación a una alarma relacionada con una instancia que no admite acciones de recuperación.

Cuando se activa la alarma `StatusCheckFailed_System` y se inicia la acción de recuperación, se le notificará mediante el tema de Amazon SNS que eligió al crear la alarma y la acción de recuperación asociada. Durante la recuperación de la instancia, la instancia se migró durante un reinicio de instancia y los datos que hay en la memoria se pierden. Cuando el proceso se ha completado, la información se publica en el tema de SNS que haya configurado para la alarma. Cualquier persona que esté suscrita a este tema de SNS recibirá una notificación por correo electrónico que incluya el estado del intento de recuperación e instrucciones adicionales. Observará un reinicio de instancia en la instancia recuperada.

> **Note**
>
> La acción de recuperación solo se puede utilizar con `StatusCheckFailed_System`, no con `StatusCheckFailed_Instance`.

Los problemas siguientes pueden provocar errores en las comprobaciones de estado del sistema:

- Pérdida de conectividad de red
- Pérdida de potencia del sistema
- Problemas de software en el host físico

- Problemas de hardware en el host físico que afectan a la accesibilidad a la red

La acción de recuperación solo se admite en instancias que cumplen determinadas características. Para obtener más información, consulte Resiliencia de las instancias.

Si la instancia tiene una dirección IP pública, la conserva tras la recuperación.

> **Important**
>
> Para evitar una condición de carrera entre las acciones de reinicio y de recuperación, evite configurar el mismo número de periodos de evaluación para una alarma de reinicio y otra de recuperación. Le recomendamos que configure las alarmas de recuperación en dos periodos de un minuto cada uno. Para obtener más información, consulte Evaluación de una alarma en la Guía del usuario de Amazon CloudWatch.

Para crear una alarma para recuperar una instancia (consola de Amazon EC2)

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancias).
3. Seleccione la instancia y elija Actions (Acciones) (Acciones), Monitoring and troubleshoot (Monitoreo y solución de problemas), Manage CloudWatch alarms (Administrar alarmas de CloudWatch).

   Alternativamente, puede elegir el signo más (

) en la columna Alarm status (Estado de alarma).
4. En la página Manage CloudWatch alarms (Administrar alarmas de CloudWatch), realice lo siguiente:

   a. Elija Create an alarm (Crear una alarma).

   b. Para recibir un correo electrónico cuando se activa la alarma, en Alarm notification (Notificación de alarma), elija un tema Amazon SNS existente. Primero debe crear un tema de Amazon SNS mediante la consola de Amazon SNS. Para obtener más información, consulte Uso de Amazon SNS para mensajería de aplicación a persona (A2P) en Guía para desarrolladores de Amazon Simple Notification Service.

> **Note**
>
> Los usuarios deben suscribirse al tema de SNS especificado para recibir notificaciones por correo electrónico cuando se active la alarma. El Usuario raíz de la cuenta de AWS siempre recibe notificaciones de correo electrónico cuando se producen acciones de recuperación automática de instancias, incluso si no se especifica un tema de SNS o el usuario raíz no está suscrito al tema de SNS especificado.

c. Cambie Alarm action (Acción de alarma) y elija Recover (Recuperar).

d. En Group samples by (Agrupar muestras por) y Type of data to sample (Tipo de datos para mostrar), elija una estadística y una métrica. En este ejemplo, elija Average (Promedio) y Status check failed: system (Comprobación de estado no superada: sistema).

e. En Consecutive period (Periodo consecutivo) y Period (Periodo), especifique el periodo de evaluación de la alarma. En este ejemplo, escriba 2 periodos consecutivos de 5 Minutes (5 minutos).

f. Amazon CloudWatch crea automáticamente un nombre de alarma para usted. Para cambiar el nombre, en Alarm name (Nombre de alarma), ingrese un nombre nuevo. Los nombres de alarma solo pueden contener caracteres ASCII.

g. Seleccione Create (Crear).

Usar la consola de Amazon CloudWatch para ver el historial de alarmas y acciones

Puede ver el historial de alarmas y de acciones en la consola de Amazon CloudWatch Amazon CloudWatch mantiene el historial de alarmas y de acciones de las últimas dos semanas.

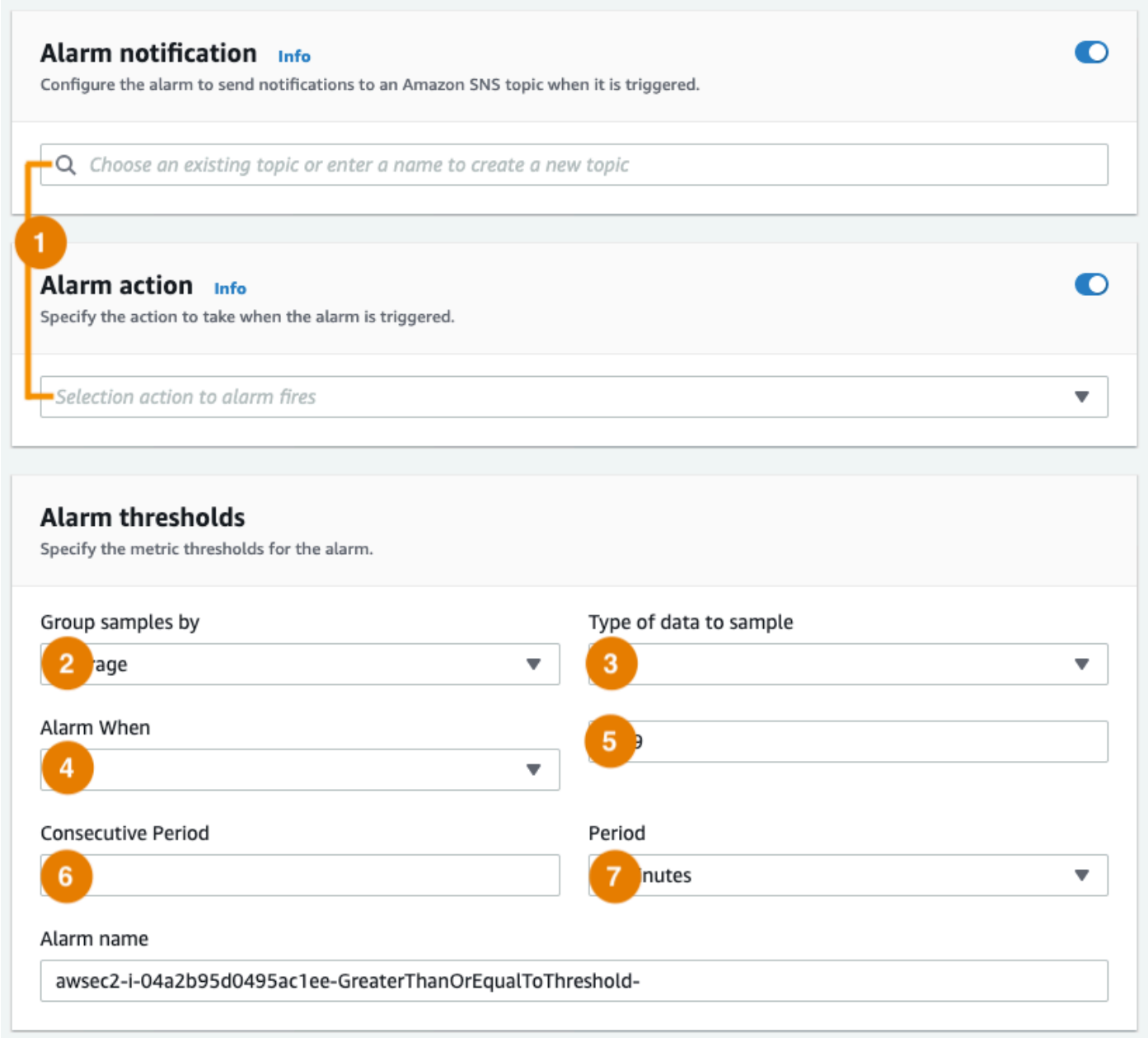
Para ver el historial de las alarmas y acciones activadas (consola de CloudWatch)

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, elija Alarms.
3. Seleccione una alarma.
4. La pestaña Details (Detalles) muestra la transición de estado más reciente junto con los valores de tiempo y las métricas.
5. Elija la pestaña History (Historial) para ver las entradas del historial más recientes.

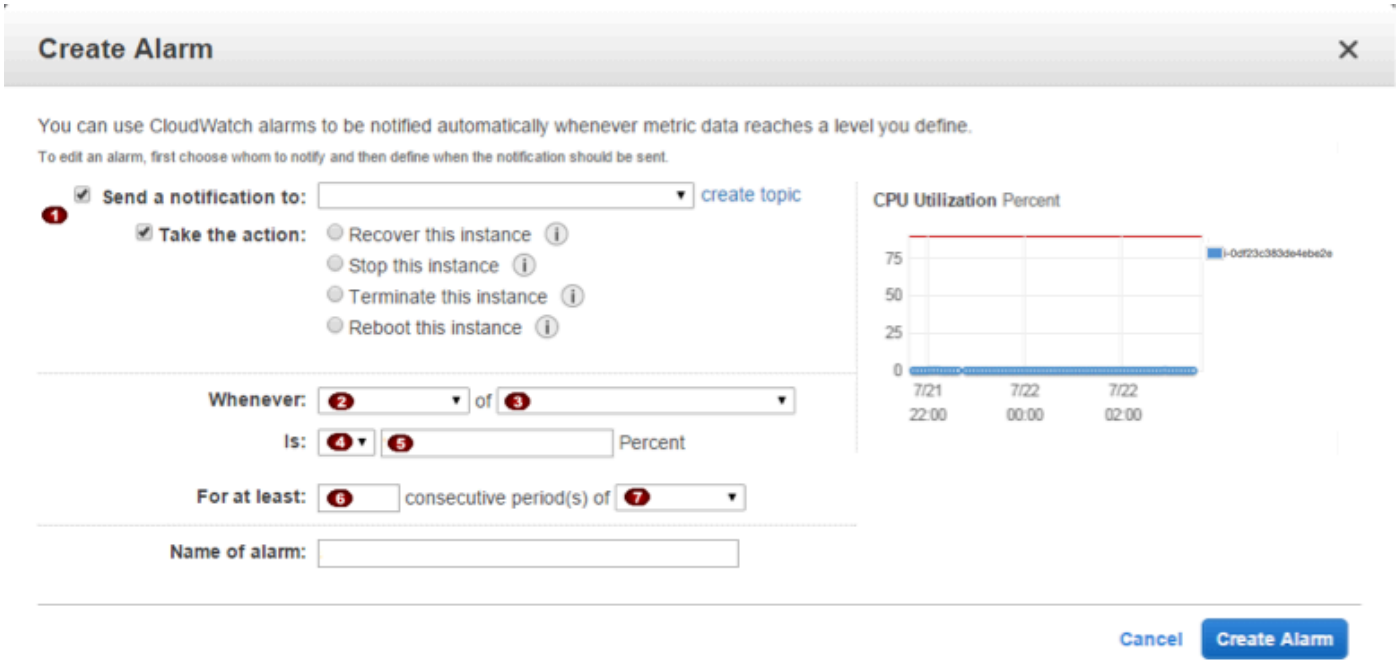
Casos de uso de acciones de alarma de Amazon CloudWatch

Puede utilizar la consola de Amazon EC2 para crear acciones de alarma que detengan o terminen una instancia Amazon EC2 cuando se cumplan determinadas condiciones. En la siguiente captura de pantalla de la página de la consola en la que se establecen las acciones de alarma, hemos enumerado estas opciones. También hemos enumerado las opciones en los escenarios que aparecen a continuación para ayudarle a crear las acciones adecuadas.

New console



Old console



Caso de uso 1: Detener instancias de desarrollo y pruebas inactivas

Crear una alarma que detenga una instancia utilizada para desarrollo o pruebas de software cuando haya estado inactiva durante al menos una hora.

Opción	Valor
1	Detener
2	Máximo
3	Utilización de la CPU
4	<=
5	10%
6	1
7	1 Hora

Caso de uso 2: Detener instancias inactivas

Crear una alarma que detenga una instancia y envíe un email cuando la instancia haya estado inactiva durante 24 horas.

Opción	Valor
1	Detener y enviar email
2	Media
3	Utilización de la CPU
4	<=
5	5%
6	24
7	1 Hora

Caso de uso 3: Enviar un email sobre servidores web con un tráfico inusualmente alto

Crear una alarma que envíe un email cuando una instancia supere los 10 GB de tráfico de red de salida al día.

Opción	Valor
1	Email
2	Sum
3	Salida de red
4	>
5	10 GB
6	24

Opción	Valor
7	1 Hora

Caso de uso 4: Detener servidores web con un tráfico inusualmente alto

Crear una alarma que detenga una instancia y envíe un mensaje de texto (SMS) si el tráfico de salida supera 1 GB por hora.

Opción	Valor
1	Detener y enviar SMS
2	Sum
3	Salida de red
4	>
5	1 GB
6	1
7	1 Hora

Escenario 5: detener una instancia deteriorada

Crear una alarma que detenga una instancia que dé error en tres comprobaciones de estado consecutivas (realizadas en intervalos de 5 minutos).

Opción	Valor
1	Detener
2	Media
3	Comprobación de estado no superada: sistema
4	-

Opción	Valor
5	-
6	1
7	15 minutos

Escenario 6: terminar instancias cuando se completen los trabajos de procesamiento por lotes

Crear una alarma que termine una instancia que ejecuta trabajos por lotes cuando ya no envía datos de resultados.

Opción	Valor
1	Finalizar
2	Máximo
3	Salida de red
4	<=
5	100,000 bytes
6	1
7	5 minutos

Automatización de Amazon EC2 con EventBridge

Amazon EventBridge puede utilizarse para automatizar los Servicios de AWS y responder automáticamente a eventos del sistema, como los problemas de disponibilidad de las aplicaciones o los cambios en los recursos. Los eventos de los servicios de AWS se envían a EventBridge casi en tiempo real. Puede crear reglas para indicar qué eventos le resultan de interés, así como qué acciones se van a realizar cuando un evento cumpla una de las reglas. Entre las acciones que se pueden activar automáticamente se incluyen las siguientes:

- Invocar una función de AWS Lambda
- Invocar Ejecutar comando de Amazon EC2
- Transmitir el evento a Amazon Kinesis Data Streams
- Activar una máquina de estado de AWS Step Functions
- Notificar un tema de Amazon SNS
- Notificar una cola de Amazon SQS

A continuación, se muestran ejemplos de cómo puede utilizar EventBridge con Amazon EC2:

- Active una función de Lambda siempre que una instancia ingrese al estado running (en ejecución).
- Notifique un tema de Amazon SNS cuando se cree o modifique un volumen de Amazon EBS.
- Envíe un comando a una o más instancias de Amazon EC2 mediante Ejecutar comando de Amazon EC2 siempre que se produzca un evento concreto en otro servicio de AWS.

Para más información, consulte la Guía del usuario de Amazon EventBridge.

Tipos de eventos de Amazon EC2

Amazon EC2 admite los siguientes tipos de eventos:

- Cambio de estado de las AMI de EC2
- Notificación de cambio de estado del lanzamiento rápido de EC2
- Error de la flota de EC2
- Información sobre la flota de EC2
- Cambio de instancia de la flota de EC2
- Cambio de solicitud de instancia de spot de la flota de EC2
- Cambio de estado de la flota de EC2
- Recomendación de reequilibrio de las instancias de EC2
- EC2 Instance State-change Notification
- Error de la flota de spot de EC2
- Información sobre la flota de spot de EC2
- Cambio de instancia de la flota de spot de EC2
- Cambio de solicitud de instancia de spot de la flota de spot de EC2

- Cambio de estado de la flota de spot de EC2
- Advertencia de interrupción de la instancia de spot de EC2
- Cumplimiento de solicitud de instancia de spot de EC2
- Notificación de infrautilización de EC2 ODCR

Para obtener información acerca de los tipos de eventos que admite Amazon EBS, consulte EventBridge para Amazon EBS.

Registro de llamadas a la API de Amazon EC2 mediante AWS CloudTrail

La API de Amazon EC2 está integrada con AWS CloudTrail, un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un Servicio de AWS. CloudTrail captura todas las llamadas a la API de Amazon EC2 como eventos, incluidas las llamadas procedentes de la consola y las llamadas de código a las operaciones de la API. Mediante la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a la API de Amazon EC2, la dirección IP desde la que se realizó, cuándo se realizó y detalles adicionales.

Para más información sobre CloudTrail, consulte la Guía del usuario de AWS CloudTrail.

Información de la API de Amazon EC2 en CloudTrail

CloudTrail se habilita en su Cuenta de AWS cuando se crea la cuenta. Cuando se produce una actividad en Amazon EC2 y en Amazon EBS, dicha actividad se registra en un evento de CloudTrail junto con otros eventos de Servicio de AWS en el Historial de eventos. Puede ver, buscar y descargar eventos recientes en su Cuenta de AWS. Para más información, consulte Visualización de eventos con el historial de eventos de CloudTrail.

Para mantener un registro continuo de los eventos en su Cuenta de AWS, incluidos los eventos de Amazon EC2 y Amazon EBS, cree un registro de seguimiento. Un registro de seguimiento permite a CloudTrail enviar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las Regiones de AWS. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. También es posible configurar otros servicios de AWS para analizar en profundidad y actuar en función de los datos de eventos recopilados en los registros de CloudTrail. Para obtener más información, consulte:

- Creación de un registro de seguimiento para su Cuenta de AWS
- Integraciones de Servicio de AWS con registros de CloudTrail
- Configuración de notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de registro de CloudTrail desde varias regiones y Recibir archivos de registro de CloudTrail desde varias cuentas

CloudTrail registra todas las acciones de Amazon EC2 y las acciones de administración de Amazon EBS, y se documentan en la Referencia de la API de Amazon EC2. Por ejemplo, las llamadas a las acciones RunInstances, DescribeInstances o CreateImage generan entradas en los archivos de registro de CloudTrail.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario lo ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales del usuario raíz o del usuario de IAM.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro Servicio de AWS.

Para obtener más información, consulte Elemento userIdentity de CloudTrail.

Introducción a las entradas del archivo de registro de la API de Amazon EC2

Un registro de seguimiento es una configuración que permite la entrega de eventos como archivos de registros en un bucket de Amazon S3 que especifique. Los archivos de registro de CloudTrail pueden contener una o varias entradas de registro. Un evento representa una solicitud específica realizada desde un origen y contiene información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. Los archivos de registro de CloudTrail no son un rastro de la stack ordenado de las llamadas a las API públicas, por lo que no aparecen en ningún orden específico.

El siguiente ejemplo de archivo de registro muestra que un usuario ha terminado una instancia.

```
{
   "Records":[
      {
         "eventVersion":"1.03",
```

```
        "userIdentity":{
           "type":"Root",
           "principalId":"123456789012",
           "arn":"arn:aws:iam::123456789012:root",
           "accountId":"123456789012",
           "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
           "userName":"user"
        },
        "eventTime":"2016-05-20T08:27:45Z",
        "eventSource":"ec2.amazonaws.com",
        "eventName":"TerminateInstances",
        "awsRegion":"us-west-2",
        "sourceIPAddress":"198.51.100.1",
        "userAgent":"aws-cli/1.10.10 Python/2.7.9 Windows/7botocore/1.4.1",
        "requestParameters":{
           "instancesSet":{
              "items":[{
                 "instanceId":"i-1a2b3c4d"
              }]
           }
        },
        "responseElements":{
           "instancesSet":{
              "items":[{
                 "instanceId":"i-1a2b3c4d",
                 "currentState":{
                    "code":32,
                    "name":"shutting-down"
                 },
                 "previousState":{
                    "code":16,
                    "name":"running"
                 }
              }]
           }
        },
        "requestID":"be112233-1ba5-4ae0-8e2b-1c302EXAMPLE",
        "eventID":"6e12345-2a4e-417c-aa78-7594fEXAMPLE",
        "eventType":"AwsApiCall",
        "recipientAccountId":"123456789012"
     }
   ]
}
```

Uso de AWS CloudTrail para auditar las conexiones mediante EC2 Instance Connect

Use AWS CloudTrail para auditar a los usuarios que se conectan a sus instancias mediante EC2 Instance Connect.

Para auditar la actividad SSH mediante EC2 Instance Connect con la consola de AWS CloudTrail

1. Abra la consola de CloudTrail en https://console.aws.amazon.com/cloudtrail/.
2. Compruebe que se encuentra en la región correcta.
3. En el panel de navegación, elija Event history (Historial de eventos).
4. En Filtro, elija Origen del evento, ec2-instance-connect.amazonaws.com.
5. De forma opcional, en Time range (Intervalo de tiempo), seleccione un intervalo de tiempo.
6. Elija el icono de Refresh events (Eventos de actualización).
7. La página muestra los eventos que se corresponden a las llamadas a la API de SendSSHPublicKey. Amplíe un evento con la flecha para ver detalles adicionales, como el nombre de usuario y la clave de acceso AWS que se empleó para realizar la conexión SSH y la dirección IP de origen.
8. Para mostrar toda la información del evento en formato JSON, elija View event (Ver evento). El campo requestParameters contiene el ID de instancia de destino, el nombre de usuario del SO y la clave pública que se emplearon para realizar la conexión SSH.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "ABCDEFGONGNOMOOCB6XYTQEXAMPLE",
        "arn": "arn:aws:iam::1234567890120:user/IAM-friendly-name",
        "accountId": "123456789012",
        "accessKeyId": "ABCDEFGUKZHNAW4OSN2AEXAMPLE",
        "userName": "IAM-friendly-name",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-09-21T21:37:58Z"}
        }
    },
    "eventTime": "2018-09-21T21:38:00Z",
```

```
    "eventSource": "ec2-instance-connect.amazonaws.com",
    "eventName": "SendSSHPublicKey ",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "123.456.789.012",
    "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
    "requestParameters": {
        "instanceId": "i-0123456789EXAMPLE",
        "osUser": "ec2-user",
        "SSHKey": {
            "publicKey": "ssh-rsa ABCDEFGHIJKLMNO01234567890EXAMPLE"
        }
     },
    "responseElements": null,
    "requestID": "1a2s3d4f-bde6-11e8-a892-f7ec64543add",
    "eventID": "1a2w3d4r5-a88f-4e28-b3bf-30161f75be34",
    "eventType": "AwsApiCall",
    "recipientAccountId": "0987654321"
}
```


Si ha configurado su cuenta de AWS para que recopile eventos de CloudTrail en un bucket de S3, puede descargar y auditar la información mediante programación. Para obtener más información, consulte Obtención y visualización de los archivos de registro de CloudTrail en la Guía del usuario de AWS CloudTrail.

Monitorear sus aplicaciones .NET y SQL Server con CloudWatch Application Insights

CloudWatch Application Insights lo ayuda a monitorear sus aplicaciones .NET y SQL Server que utilizan instancias de Amazon EC2 junto con otros recursos de aplicaciones de AWS. Identifica y configura registros de métricas clave y alarmas para los recursos y la pila de tecnología de la aplicación (como la base de datos Microsoft SQL Server, los servidores web (IIS) y de aplicaciones, el sistema operativo, los balanceadores de carga y las colas). Controla continuamente las métricas y los registros para detectar y relacionar anomalías y errores. Cuando se detectan errores y anomalías, Application Insights genera eventos de CloudWatch que puede utilizar para configurar notificaciones o realizar acciones. Para ayudar con la solución de problemas, crea paneles automatizados para los problemas detectados, que incluyen anomalías de métricas y errores de registro relacionados, además de información adicional que indica la posible causa raíz. Los paneles automatizados lo

ayudan a adoptar rápidamente medidas correctivas para mantener sus aplicaciones en buen estado y para evitar que los usuarios finales de la aplicación se vean afectados.

Para ver una lista completa de registros y métricas compatibles, consulte Registros y métricas compatibles con Amazon CloudWatch Application Insights.

Información proporcionada sobre los problemas detectados

- Un breve resumen del problema
- La hora de inicio y la fecha del problema
- La gravedad del problema: alta/media/baja
- El estado del problema detectado: en curso/resuelto
- Información: información generada automáticamente sobre el problema detectado y su posible causa raíz
- Comentarios sobre la información: los comentarios que usted ha proporcionado sobre la utilidad de la información generada por CloudWatch Application Insights para .NET y SQL Server
- Observaciones relacionadas: una vista detallada de las anomalías de las métricas y fragmentos de errores de los registros pertinentes relacionados con el problema en los distintos componentes de la aplicación

Comentarios

Puede proporcionar comentarios sobre la información generada automáticamente relativa a los problemas detectados indicando si es útil o no es útil. Sus comentarios sobre la información, junto con los diagnósticos de la aplicación (anomalías de métricas y excepciones de registro), se utilizan para mejorar la detección de problemas similares en el futuro.

Para obtener más información, consulte la documentación de CloudWatch Application Insights en la Guía del usuario de Amazon CloudWatch.

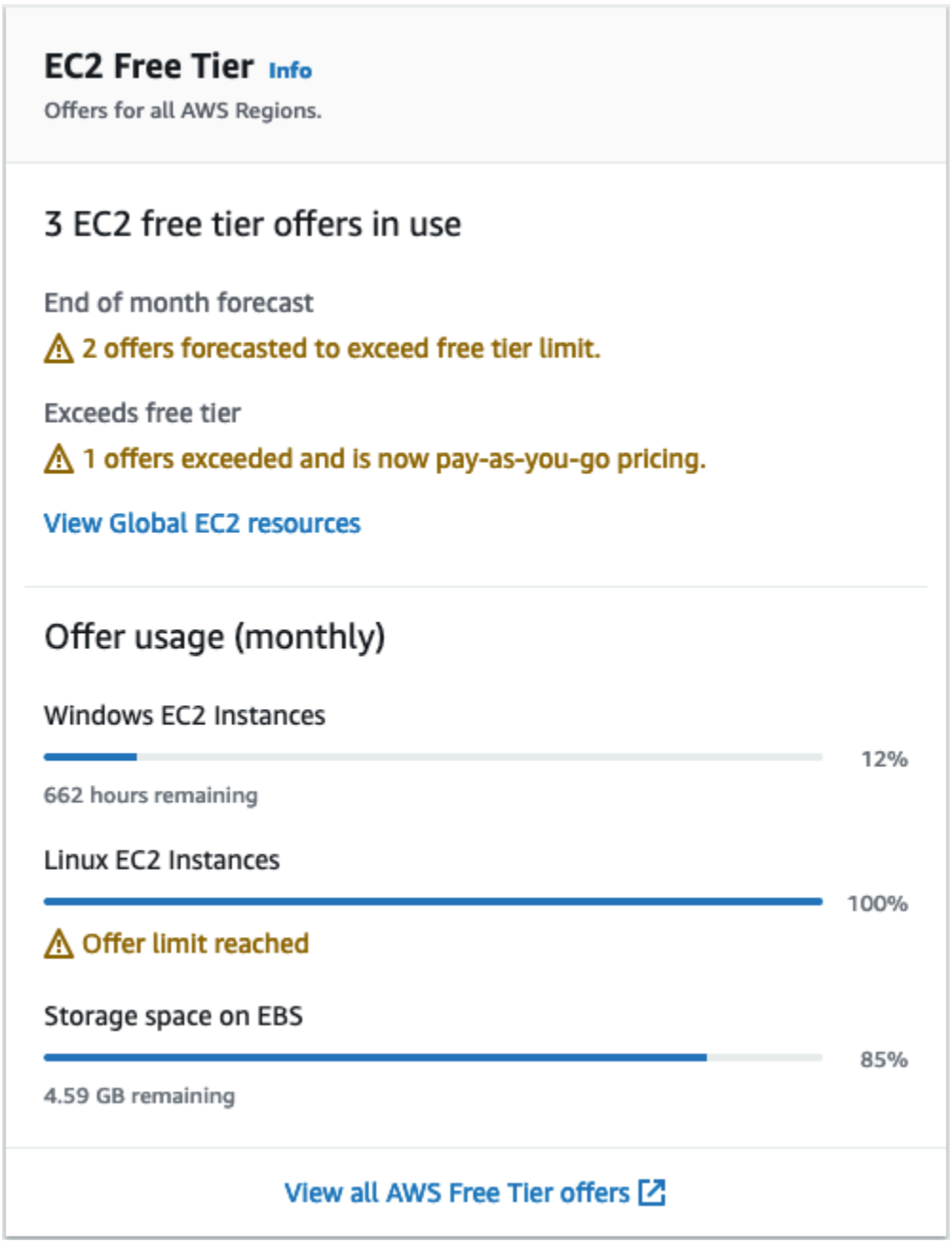
Seguimiento del uso del nivel gratuito para Amazon EC2

Puede usar Amazon EC2 sin incurrir en cargos si lleva siendo cliente de AWS menos de 12 meses y se mantiene dentro de los límites de uso del capa gratuita de AWS. Es importante hacer un seguimiento del uso del nivel gratuito para evitar sorpresas en la facturación. Si supera los límites del nivel gratuito, incurrirá en los cargos estándar de pago por uso.

> **Note**
>
> Si lleva siendo cliente de AWS más de 12 meses, ya no podrá utilizar el nivel gratuito y no verá el cuadro Nivel gratuito de EC2 que se describe en el siguiente procedimiento.

Seguimiento del uso del nivel gratuito

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija EC2 Dashboard (Panel EC2).
3. Busque el cuadro Nivel gratuito de EC2 (en la parte superior derecha).



4. En el cuadro Nivel gratuito de EC2, compruebe el uso del nivel gratuito de la siguiente manera:

   - En Ofertas del nivel gratuito de EC2 en uso, tenga en cuenta las advertencias:
     - Previsión de fin de mes: le advierte de que se le cobrarán cargos este mes si continúa con su patrón de uso actual.
     - Supera el nivel gratuito: le advierte de que ha superado los límites del nivel gratuito y que ya está incurriendo en cargos.

- En Uso de la oferta (mensual), anote el uso que hace de las instancias de Linux, las instancias de Windows y el almacenamiento de EBS. El porcentaje indica qué parte de los límites del nivel gratuito ha utilizado este mes. Si está al 100 %, incurrirá en cargos por el uso posterior.

> **Note**
>
> Esta información solo aparece después de haber creado una instancia. Sin embargo, la información de uso no se actualiza en tiempo real, sino que se actualiza tres veces al día.

5. Para evitar incurrir en más cargos, elimine todos los recursos que estén incurriendo en cargos ahora o que van a incurrir si supera el límite de uso del nivel gratuito.

   - Para obtener instrucciones sobre cómo eliminar la instancia, vaya al siguiente paso de este tutorial.
   - Para comprobar si tiene recursos en otras regiones que podrían estar incurriendo en cargos, en el cuadro Nivel gratuito de EC2, seleccione Ver recursos globales de EC2 para abrir EC2 Global View. Para obtener más información, consulte Amazon EC2 Global View.

6. Para ver el uso de los recursos de todos los Servicios de AWS en el capa gratuita de AWS, en la parte inferior del cuadro Nivel gratuito de EC2, seleccione Ver todas las ofertas del capa gratuita de AWS. Para obtener más información, consulte Utilización del nivel gratuito de capa gratuita de AWS en la Guía del usuario de facturación de AWS.

Redes en Amazon EC2

Amazon VPC le permite iniciar recursos de AWS, como instancias de Amazon EC2, en una red virtual dedicada a la cuenta de AWS, conocida como nube privada virtual (VPC). Al iniciar una instancia, puede seleccionar una subred de la VPC. La instancia está configurada con una interfaz de red principal, que es una tarjeta de red virtual lógica. La instancia recibe una dirección IP privada principal de la dirección IPv4 de la subred y se asigna a la interfaz de red principal.

Puede controlar si la instancia recibe una dirección IP pública del grupo de direcciones IP públicas de Amazon. La dirección IP pública de una instancia se asocia a su instancia solo hasta que se detenga o finalice. Si necesita una dirección IP pública persistente, puede asignar una dirección IP elástica para su cuenta AWS y asociarla con una instancia o una interfaz de red. Una dirección IP elástica permanece asociada a su cuenta AWS hasta que la libere, y puede moverla de una instancia a otra según sea necesario. Puede traer su propio intervalo de direcciones IP a su cuenta AWS, donde aparece como un grupo de direcciones y, a continuación, asignar direcciones IP elásticas desde su grupo de direcciones.

Para aumentar el rendimiento de la red y reducir la latencia, puede iniciar instancias en un grupo de ubicación. Puede obtener un Packet Per Second (PPS, Rendimiento de paquete por segundo) significativamente mayor utilizando una red mejorada. Puede acelerar las aplicaciones de informática y machine learning de alto rendimiento mediante un Elastic Fabric Adapter (EFA), que es un dispositivo de red que se puede conectar a un tipo de instancia compatible.

Características

- Regiones y zonas
- Direccionamiento IP de instancias Amazon EC2
- Tipos de nombres de host de instancias de Amazon EC2
- Traiga sus propias direcciones IP (BYOIP) en Amazon EC2
- Direcciones IP elásticas
- Interfaces de red elásticas
- Ancho de banda de red de instancias de Amazon EC2
- Redes mejoradas en Amazon EC2
- Elastic Fabric Adapter
- Topología de instancias de Amazon EC2

- Grupos de ubicación
- Unidad de transmisión máxima (MTU) de red de la instancia de EC2
- Nubes privadas virtuales para sus instancias EC2

Regiones y zonas

Amazon EC2 está alojado en varias ubicaciones de todo el mundo. Estas ubicaciones se componen de Regiones de AWS, zonas de disponibilidad, locales AWS Outposts y de Wavelength.

- Cada región es un área geográfica independiente.
- Las zonas de disponibilidad son varias ubicaciones aisladas dentro de cada región.
- Las Local Zones le proporcionan la capacidad de colocar recursos, como por ejemplo de computación y de almacenamiento, en varias ubicaciones más cercanas a los usuarios finales.
- AWS Outposts brinda servicios, infraestructura y modelos operativos nativos de AWS a prácticamente cualquier centro de datos, espacio de coubicación o instalación en las instalaciones.
- Las zonas de Wavelength permiten a los desarrolladores crear aplicaciones que ofrecen latencia extremadamente baja para dispositivos 5G y usuarios finales. Wavelength implementa servicios de computación y almacenamiento de AWS estándar al borde de redes 5G de operadores de telecomunicaciones.

AWS opera centros de datos con tecnología de vanguardia y alta disponibilidad. Aunque es infrecuente, puede suceder que se produzcan errores que afecten a la disponibilidad de las instancias que están en la misma ubicación. Si aloja todas las instancias en una misma ubicación y se produce un error en ella, ninguna de las instancias estaría disponible.

Para ayudarlo a determinar qué implementación es la mejor para usted, consulte Preguntas frecuentes de AWS Wavelength.

Contenido

- Regiones
- Zonas de disponibilidad
- Local Zones
- Zonas de Wavelength
- AWS Outposts

Regiones

Cada región se ha diseñado para que esté totalmente aislada de las demás regiones. Con ello se consigue la mejor tolerancia a errores y estabilidad posibles.

Cuando se consultan los recursos, solo se ven los recursos vinculados a la región especificada. Esto se debe a que las regiones están aisladas entre sí y no replicamos automáticamente los recursos en distintas regiones.

Cuando inicia una instancia, debe seleccionar una AMI que esté en la misma región. Si la AMI está en otra región, puede copiar la AMI a la región que está usando. Para obtener más información, consulte Copiar una AMI.

Tenga en cuenta que existe un cargo por transferencia de datos entre regiones. Para obtener más información, consulte Precios de Amazon EC2: transferencia de datos.

Contenido

Regiones disponibles

Su cuenta determina las regiones que están disponibles para usted.

- Una Cuenta de AWS proporciona varias regiones de manera que se puedan iniciar instancias de Amazon EC2 en ubicaciones que cumplan sus requisitos. Por ejemplo, podría desear iniciar instancias en Europa, para estar más cerca de sus clientes europeos o para cumplir requisitos legales.
- Una cuenta de AWS GovCloud (Oeste de EE. UU.) proporciona acceso a la región de AWS GovCloud (Oeste de EE. UU.) y la región de AWS GovCloud (Este de EE. UU.). Para obtener más información, consulte AWS GovCloud (US).
- Una cuenta de Amazon AWS (China) proporciona acceso solo a las regiones de Pekín y Ningxia. Para obtener más información, consulte Amazon Web Services en China.

En la siguiente tabla se muestran las regiones proporcionadas por una Cuenta de AWS. No puede describir ni obtener acceso a regiones adicionales desde una Cuenta de AWS, como las AWS GovCloud (US) Regions o las regiones de China. Para utilizar una región introducida después del 20 de marzo de 2019, debe habilitar la región. Para obtener más información, consulte Especificar qué regiones de AWS puede utilizar su cuenta en la Guía de referencia de AWS Account Management.

Code	Nombre	Estado de inscripción
us-east-2	Este de EE. UU. (Ohio)	No se necesita
us-east-1	EE.UU. Este (Virginia)	No obligatorio
us-west-1	Oeste de EE. UU. (Norte de California)	No obligatorio
us-west-2	EE. UU. Oeste (Oregón)	No obligatorio
af-south-1	África (Ciudad del Cabo)	Obligatoria
ap-east-1	Asia-Pacífico (Hong Kong)	Obligatoria
ap-south-2	Asia-Pacífico (Hyderabad)	Obligatoria
ap-southeast-3	Asia-Pacífico (Yakarta)	Obligatoria
ap-southeast-4	Asia-Pacífico (Melbourne)	Obligatoria
ap-south-1	Asia-Pacífico (Bombay)	No obligatorio
ap-northeast-3	Asia-Pacífico (Osaka)	No obligatorio
ap-northeast-2	Asia-Pacífico (Seúl)	No obligatorio
ap-southeast-1	Asia-Pacífico (Singapur)	No obligatorio
ap-southeast-2	Asia-Pacífico (Sídney)	No obligatorio
ap-northeast-1	Asia-Pacífico (Tokio)	No obligatorio
ca-central-1	Canadá (centro)	No obligatorio
ca-west-1	Oeste de Canadá (Calgary)	Obligatoria

Code	Nombre	Estado de inscripción
eu-central-1	Europa (Fráncfort)	No obligatorio
eu-west-1	Europa (Irlanda)	No obligatorio
eu-west-2	Europa (Londres)	No obligatorio
eu-south-1	Europa (Milán)	Obligatoria
eu-west-3	Europa (París)	No obligatorio
eu-south-2	Europa (España)	Obligatoria
eu-north-1	Europa (Estocolmo)	No obligatorio
eu-central-2	Europa (Zúrich)	Obligatoria
il-central-1	Israel (Tel Aviv)	Obligatoria
me-south-1	Medio Oriente (Baréin)	Obligatoria
me-central-1	Medio Oriente (EAU)	Obligatoria
sa-east-1	América del Sur (São Paulo)	No se necesita

Para obtener más información, consulte Infraestructura global de AWS.

El número y la asignación de zonas disponibles según la región puede variar entre Cuentas de AWS. Para obtener una lista de las zonas de disponibilidad que están disponibles para su cuenta, puede usar la consola de Amazon EC2 o la interfaz de línea de comandos. Para obtener más información, consulte Describir sus regiones.

Regiones y puntos de enlace

Cuando trabaja con una instancia usando la interfaz de línea de comandos o las acciones de API, debe especificar el punto de conexión regional. Para obtener más información acerca de las regiones y los puntos de conexión para Amazon EC2, consulte Puntos de conexión y cuotas de Amazon EC2 en Referencia general de Amazon Web Services.

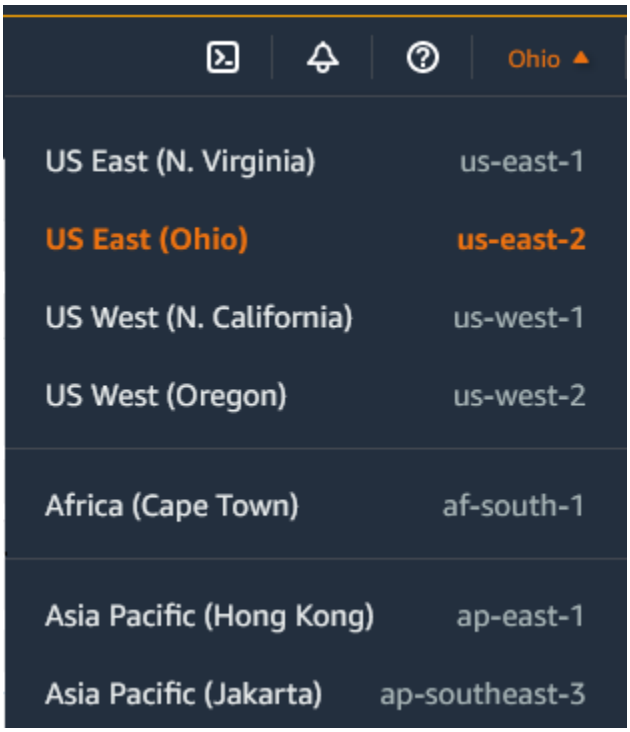
Para obtener más información sobre los puntos de conexión y los protocolos en AWS GovCloud (Oeste de EE. UU.), consulte Puntos de conexión en la Guía de usuario de AWS GovCloud (US).

Describir sus regiones

Puede usar la consola de Amazon EC2 o la interfaz de línea de comandos para determinar qué regiones están disponibles para su cuenta. Para obtener más información acerca de estas interfaces de línea de comandos, consulte Acceder a Amazon EC2.

Para encontrar las regiones mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la barra de navegación, seleccione el selector Regions (Regiones).



3. Los recursos de EC2 para esta región se muestran en el Panel de EC2 en la sección Recursos.

Para encontrar las regiones mediante la AWS CLI

Use el comando describe-regions como se indica a continuación para describir las regiones que están habilitadas para su cuenta.

```
aws ec2 describe-regions
```

Para describir todas las regiones, incluidas las regiones que están deshabilitadas para su cuenta, agregue la opción `--all-regions` como se indica a continuación.

```
aws ec2 describe-regions --all-regions
```

Obtenga el nombre para mostrar de la región

Puedes usar el almacén de parámetros de AWS Systems Manager para ver el nombre mostrado de una región. Cada región tiene parámetros públicos en la siguiente ruta.

```
/aws/service/global-infrastructure/regions/region-code
```

Los parámetros públicos de una región incluyen lo siguiente:

- /aws/service/global-infrastructure/regions/*region-code*/domain
- /aws/service/global-infrastructure/regions/*region-code*/geolocationCountry
- /aws/service/global-infrastructure/regions/*region-code*/geolocationRegion
- /aws/service/global-infrastructure/regions/*region-code*/longName
- /aws/service/global-infrastructure/regions/*region-code*/partition

El parámetro `longName` contiene el nombre para mostrar de la región. El siguiente comando get-parameters-by-path devuelve el nombre para mostrar de la región `af-south-1`. Utiliza la opción `--query` para limitar la salida al nombre de la región. En Linux, debe escribir la cadena de consulta entre comillas simples. Para ejecutar este comando mediante la línea de comandos de Windows, omita las comillas simples o cámbielas por comillas dobles.

AWS CLI on Linux

```
aws ssm get-parameters-by-path \
    --path /aws/service/global-infrastructure/regions/af-south-1 \
    --query 'Parameters[?Name.contains(@,`longName`)].Value' \
    --output text
```

AWS CLI on Windows

```
aws ssm get-parameters-by-path ^
    --path /aws/service/global-infrastructure/regions/af-south-1 ^
```

```
    --query "Parameters[?Name.contains(@,`longName`)].Value" ^
    --output text
```

Tools for PowerShell

Si no está instalado, instale el módulo AWS.Tools.SimpleSystemsManagement en las herramientas para PowerShell al ejecutar `Install-AWSToolsModule AWS.Tools.SimpleSystemsManagement -CleanUp`.

```
$parameterPath = "/aws/service/global-infrastructure/regions/af-south-1"
$substringToMatch = "longName"
$filteredParameters = Get-SSMParametersByPath -Path $parameterPath `
| Where-Object { $_.Name -like "*$substringToMatch*" } `
| ForEach-Object { Write-Output $_.Value }
$filteredParameters
```

A continuación, se muestra un ejemplo del resultado.

```
Africa (Cape Town)
```

Para obtener más información, consulte Trabajar con parámetros públicos en la Guía del usuario de AWS Systems Manager.

Especificar la región para un recurso

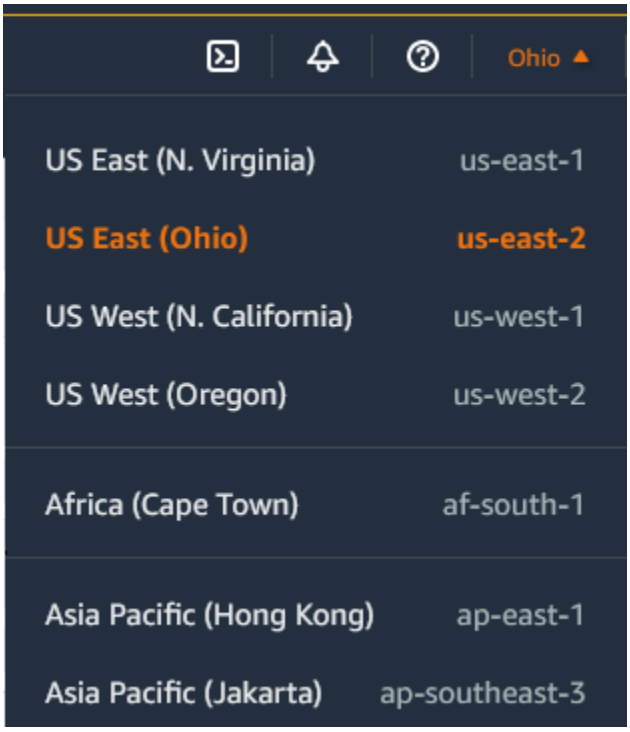
Cada vez que crea un recurso de Amazon EC2, puede especificar la región para el recurso. Puede especificar la región para un recurso mediante la AWS Management Console o la línea de comandos.

Consideraciones

Es posible que algunos recursos de AWS no estén disponibles en todas las regiones. Asegúrese de que puede crear los recursos que necesita en las regiones deseadas antes de iniciar una instancia.

Para especificar la región para un recurso mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la barra de navegación, seleccione el selector Regions y, a continuación, seleccione la región.



Para especificar la región predeterminada mediante la línea de comandos

Puede establecer el valor de una variable de entorno en el punto de conexión regional deseado (por ejemplo, `https://ec2.us-east-2.amazonaws.com`):

- `AWS_DEFAULT_REGION` (AWS CLI)
- `Set-AWSDefaultRegion` (AWS Tools for Windows PowerShell)

También puede utilizar la opción de la línea de comandos `--region` (AWS CLI) o `-Region` (AWS Tools for Windows PowerShell) con cada comando. Por ejemplo, `--region us-east-2`.

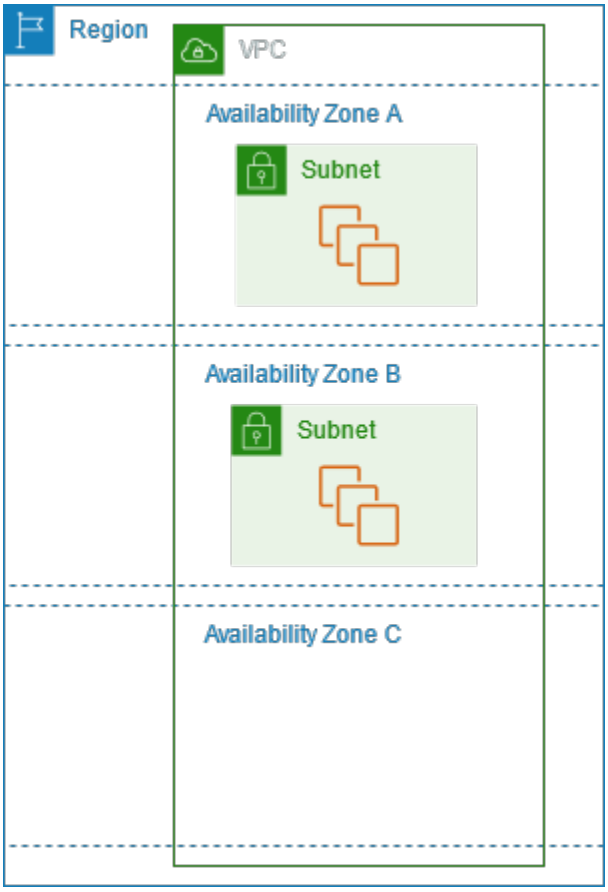
Para obtener más información acerca de los puntos de conexión para Amazon EC2, consulte Puntos de conexión y cuotas de Amazon EC2 en la Referencia general de AWS.

Zonas de disponibilidad

Cada región tiene varias ubicaciones aisladas conocidas como zonas de disponibilidad. El código de la zona de disponibilidad es el código de la región seguido de un identificador de letra. Por ejemplo, `us-east-1a`.

Cuando inicia una instancia, debe seleccionar una región y una nube virtual privada (VPC) y, a continuación, puede seleccionar una subred de una de las zonas de disponibilidad o dejarnos elegir una por usted. Si distribuye las instancias entre varias zonas de disponibilidad y una de las instancias genera un error, puede diseñar la aplicación de forma que una instancia en otra zona de disponibilidad pueda gestionar las solicitudes. También puede usar direcciones IP elásticas para enmascarar los errores de una instancia en una zona de disponibilidad volviendo a mapear rápidamente la dirección hacia una instancia en otra zona de disponibilidad.

El siguiente diagrama ilustra varias zonas de disponibilidad en una región de AWS. La zona de disponibilidad A y la zona de disponibilidad B tienen una subred cada una y cada subred tiene instancias. La zona de disponibilidad C no tiene subredes, por lo que no se pueden iniciar instancias en esta zona de disponibilidad.



A medida que las zonas de disponibilidad crecen a lo largo del tiempo, nuestra capacidad de ampliarlas podría verse limitada. Si esto sucediera, podríamos restringir la inicialización de instancias en una zona de disponibilidad limitada, a menos que ya tuviera una instancia en dicha zona de disponibilidad. Con el tiempo, también podríamos quitar la zona de disponibilidad limitada de la lista de zonas de disponibilidad de las nuevas cuentas. Por consiguiente, una cuenta podría tener un número diferente de zonas de disponibilidad disponibles en una región que otra cuenta.

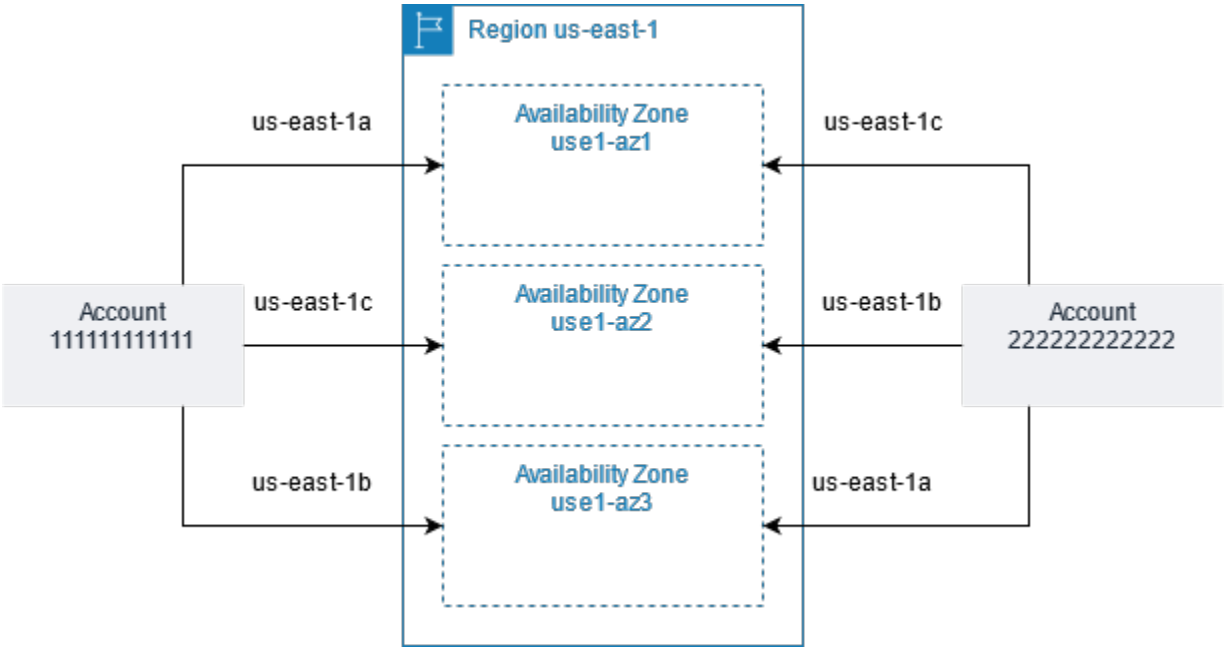
Contenido

ID de AZ

Para garantizar que los recursos se distribuyan por todas las zonas de disponibilidad de una región, asignamos zonas de disponibilidad de manera independiente a códigos de cada Cuenta de AWS en nuestras regiones más antiguas. Por ejemplo, es posible que `us-east-1a` de su Cuenta de AWS no se encuentre en la misma ubicación física que `us-east-1a` para otra Cuenta de AWS.

Para coordinar las zonas de disponibilidad entre cuentas de todas las regiones, incluso las que asignan zonas de disponibilidad, debe usar los ID de AZ (Zonas de disponibilidad), que son identificadores únicos y constantes de una zona de disponibilidad. Por ejemplo, `use1-az1` es un ID de zona de disponibilidad de la región `us-east-1` y tiene la misma ubicación física en cada Cuenta de AWS. Puede consultar los ID de las zonas de disponibilidad de su cuenta para determinar la ubicación física de sus recursos en relación con los recursos de otra cuenta. Por ejemplo, si comparte una subred en la zona de disponibilidad con el ID de AZ `use1-az2` con otra cuenta, esta subred está disponible para dicha cuenta de la zona de disponibilidad cuyo ID de zona de disponibilidad es también `use1-az2`.

En el siguiente diagrama, se ilustran dos cuentas con asignaciones diferentes del código de zona de disponibilidad para el ID de zona de disponibilidad.



Describir las zonas de disponibilidad

Puede usar la consola de Amazon EC2 o la interfaz de línea de comandos para determinar qué zonas de disponibilidad están disponibles para su cuenta. Para obtener más información acerca de estas interfaces de línea de comandos, consulte Acceder a Amazon EC2.

Para encontrar las zonas de disponibilidad mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la barra de navegación, seleccione el selector Regiones y, a continuación, seleccione la región.
3. En el panel de navegación, elija Panel de EC2.
4. Las zonas de disponibilidad se muestran en el panel Estado de los servicios.

Para encontrar las zonas de disponibilidad mediante la AWS CLI

- Utilice el comando describe-availability-zones, tal y como se indica a continuación, para describir las zonas de disponibilidad dentro de la región especificada que están habilitadas para su cuenta.

```
aws ec2 describe-availability-zones --region region-name
```

- Utilice el comando describe-availability-zones como se indica a continuación, para describir las zonas de disponibilidad con independencia del estado de inscripción.

```
aws ec2 describe-availability-zones --all-availability-zones
```

Iniciar instancias en una zona de disponibilidad

Cuando lance una instancia, seleccione una región que coloque sus instancias cerca de determinados clientes, o que cumpla los requisitos legales o de otra índole que tenga. Al iniciar instancias en distintas zonas de disponibilidad, puede proteger sus aplicaciones de los errores que se produzcan en una única ubicación.

Cuando inicia una instancia, opcionalmente puede especificar una zona de disponibilidad en la región que está usando. Si no especifica una zona de disponibilidad, seleccionamos una zona de disponibilidad por usted. Cuando inicie sus instancias iniciales, le recomendamos que acepte la zona de disponibilidad predeterminada, porque esto nos permite seleccionar la mejor zona de disponibilidad para usted en función del estado del sistema y de la capacidad disponible. Si inicia instancias adicionales, especifique una zona de disponibilidad únicamente si las nuevas instancias deben estar cerca o separadas de las instancias en ejecución.

Migrar una instancia a otra zona de disponibilidad

Si es necesario, puede migrar una instancia de una zona de disponibilidad a otra. Por ejemplo, si intenta modificar el tipo de instancia de su instancia y no podemos iniciar una instancia del nuevo tipo en la zona de disponibilidad actual, puede migrar la instancia a una zona de disponibilidad con capacidad para el nuevo tipo de instancia.

El proceso de migración implica:

- Crear una AMI a partir de la instancia original
- Iniciar una instancia en la nueva zona de disponibilidad
- Actualizar la configuración de la nueva instancia, como se muestra en el siguiente procedimiento

Para migrar una instancia a otra zona de disponibilidad

1. Cree una AMI a partir de la instancia. El procedimiento dependerá del tipo de volumen de dispositivo raíz de la instancia. Para obtener más información, consulte la documentación que corresponde al volumen de dispositivo raíz:

   - Creación de una AMI basada en Amazon EBS

- Crear una AMI de Linux con respaldo en el almacén de instancias

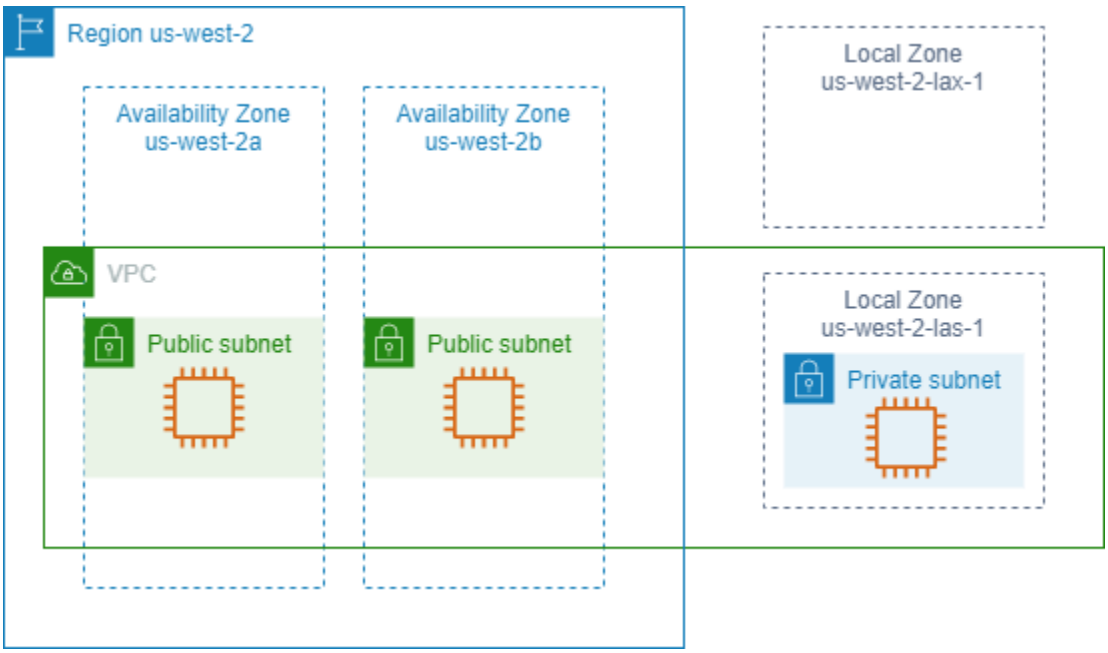
2. Si necesita conservar la dirección IPv4 privada de la instancia, debe eliminar la subred en la zona de disponibilidad actual y, a continuación, crear una subred en la zona de disponibilidad nueva con el mismo rango de direcciones IPv4 que la subred original. Tenga en cuenta que debe terminar todas las instancias en una subred antes de poder eliminarla. Por consiguiente, debería crear las AMI a partir de todas las instancias de la subred de forma que pueda mover todas las instancias de la subred actual a la nueva subred.
3. Lance una instancia desde la AMI que acaba de crear, especificando la nueva zona de disponibilidad o subred. Puede usar el mismo tipo de instancia que la instancia original o seleccionar un nuevo tipo de instancia. Para obtener más información, consulte Iniciar instancias en una zona de disponibilidad.
4. Si la instancia original tenía una dirección IP elástica asociada, asóciela con la nueva instancia. Para obtener más información, consulte Anulación de la asociación de una dirección IP elástica.
5. Si la instancia original es una instancia reservada, cambie la zona de disponibilidad de la reserva. (Si también cambió el tipo de instancia, también podrá cambiar el tipo de instancia de la reserva). Para obtener más información, consulte Enviar solicitudes de modificación.
6. (Opcional) Termine la instancia original. Para obtener más información, consulte Finalizar una instancia.

Local Zones

Una zona local es una extensión de una región de AWS que se encuentra geográficamente cerca de los usuarios. Las zonas locales tienen sus propias conexiones a Internet y son compatibles con AWS Direct Connect, por lo que los recursos creados en una zona local pueden brindar a los usuarios locales comunicaciones de baja latencia. Para obtener más información, consulte la sección ¿Qué son las zonas locales de AWS? en la Guía del usuario de zonas locales de AWS.

El código de una zona local es el código de su región seguido de un identificador que indica su ubicación física. Por ejemplo, `us-west-2-lax-1` en Los Ángeles.

En el siguiente diagrama, se ilustran la región `us-west-2` de AWS, dos de sus zonas de disponibilidad y dos de sus zonas locales. La VPC abarca las zonas de disponibilidad y una de las zonas locales. Cada zona de la VPC tiene una subred y cada subred tiene una instancia.



Para utilizar una Local Zone, primero debe habilitarla. Para obtener más información, consulte the section called “Optar por Local Zones”. A continuación, cree una subred en la zona local. Por último, inicie los recursos en la subred de la zona local, como las instancias, para que las aplicaciones estén más cerca de los usuarios.

Contenido

Local Zones disponibles

Puede utilizar la consola de Amazon EC2 o la interfaz de línea de comandos para determinar qué zonas locales están disponibles para su cuenta. Para obtener una lista completa, consulte Ubicaciones de zonas locales de AWS.

Para encontrar las Local Zones mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la barra de navegación, seleccione el selector Regions y, a continuación, seleccione la región.
3. En el panel de navegación, elija Panel de EC2.

4. En la esquina superior derecha de la página, elija Atributos de cuenta, Zonas.

Para encontrar las zonas locales con la AWS CLI

Utilice el comando describe-availability-zones, tal y como se muestra a continuación, para describir las zonas locales en la región especificada, incluso si no están habilitadas. Para describir solo las zonas locales que ha habilitado, omita la opción `--all-availability-zones`.

```
aws ec2 describe-availability-zones --region region-name --filters Name=zone-
type,Values=local-zone --all-availability-zones
```

Optar por Local Zones

Antes de especificar una Local Zone para un recurso o servicio, debe optar por Local Zones.

Consideración

Es posible que algunos recursos de AWS no estén disponibles en todas las regiones. Asegúrese de que puede crear los recursos que necesita en las regiones o Local Zones deseadas antes de iniciar una instancia en una Local Zone específica. Para obtener una lista de los servicios compatibles con cada zona local, consulte Características de zonas locales de AWS.

Para optar por Local Zones mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la esquina superior izquierda de la página, seleccione Nueva experiencia de EC2. No puede completar esta tarea utilizando la experiencia de consola anterior.
3. En la barra de navegación, seleccione el selector Regiones y, a continuación, seleccione la región.
4. En el panel de navegación, elija Panel de EC2.
5. En la esquina superior derecha de la página, elija Atributos de cuenta, Zonas.
6. Elija una zona local y seleccione Acción > Administrar grupo de zonas.
7. En Estado de suscripción, elija Habilitado.
8. Elija Actualizar.

Para optar por las zonas locales con la AWS CLI

Utilice el comando modify-availability-zone-group.

iniciar instancias en una Local Zone

Cuando lance una instancia, podrá especificar una subred que se encuentre en una Local Zone. También puede asignar una dirección IP desde un grupo de bordes de red. Un grupo de bordes de red es un conjunto único de zonas de disponibilidad, Local Zones o zonas de Wavelength desde las que AWS anuncia direcciones IP, como, por ejemplo, `us-west-2-lax-1a`.

Puede asignar las siguientes direcciones IP desde un grupo de perímetros de red:

- Direcciones IPv4 elásticas proporcionadas por Amazon
- Direcciones IPv6 de VPC proporcionadas por Amazon (disponibles solo en las zonas de Los Ángeles)

Para obtener más información sobre cómo iniciar una instancia en una Zona local, consulte Introducción a Zonas locales de AWS en la Guía del usuario de Zonas locales de AWS.

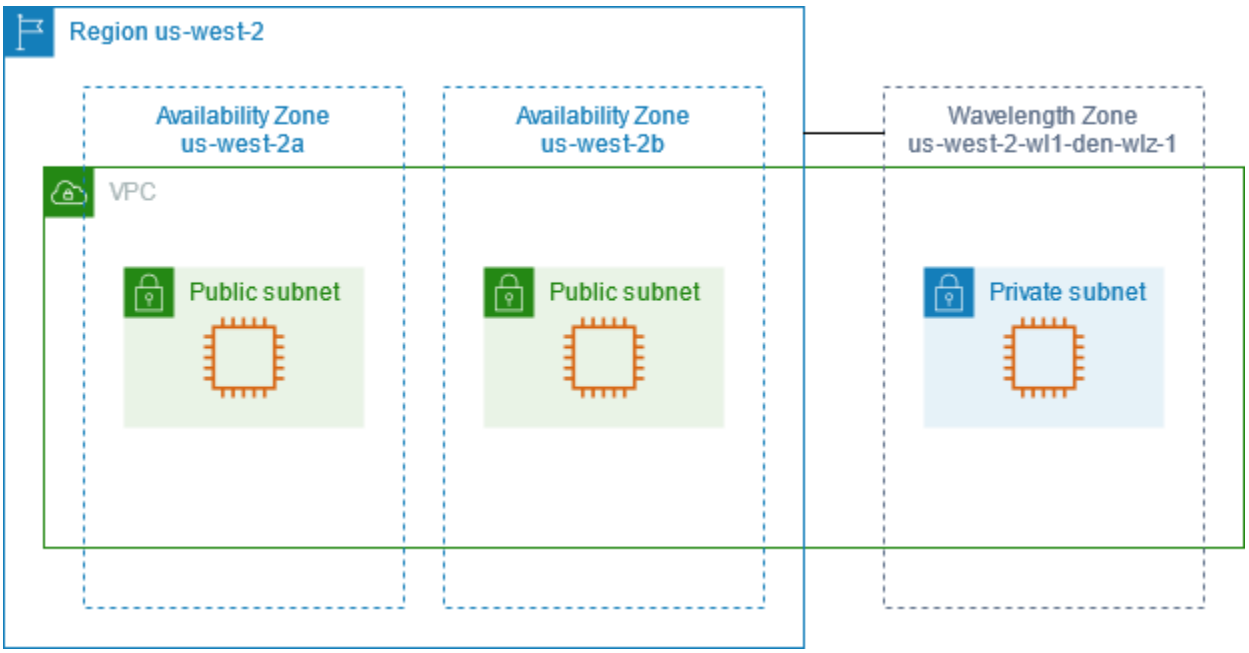
Zonas de Wavelength

AWS Wavelength permite a los desarrolladores crear aplicaciones que ofrecen una latencia extremadamente baja para dispositivos móviles y usuarios finales. Wavelength implementa servicios de computación y almacenamiento de AWS estándar al borde de redes 5G de operadores de telecomunicaciones. Los desarrolladores pueden ampliar una nube privada virtual (VPC) a una o varias zonas de Wavelength y, a continuación, utilizar recursos de AWS como instancias de Amazon EC2 para ejecutar aplicaciones que requieren una latencia extremadamente baja y una conexión a los servicios de AWS en la región.

Una zona de Wavelength es una zona aislada en la ubicación del operador donde se implementa la infraestructura de Wavelength. Las zonas de Wavelength están vinculadas a una región. Una zona de Wavelength es una extensión lógica de una región y está administrada por el plano de control de la región.

El código de una zona Wavelength es el código de su región seguido de un identificador que indica la ubicación física. Por ejemplo, `us-east-1-wl1-bos-wlz-1` en Boston.

En el siguiente diagrama, se ilustran la región `us-west-2` de AWS, dos de sus zonas de disponibilidad y una zona Wavelength. La VPC abarca las zonas de disponibilidad y la zona Wavelength. Cada zona de la VPC tiene una subred y cada subred tiene una instancia.



Para utilizar una zona de Wavelength, primero debe darse de alta en la zona. Para obtener más información, consulte the section called “Habilitar zonas de Wavelength”. A continuación, cree una subred en la zona de Wavelength. Finalmente, lance los recursos en la subred de zonas de Wavelength, de modo que las aplicaciones estén más cerca de los usuarios finales.

Las zonas de Wavelength no están disponibles en todas las regiones. Para obtener información sobre las regiones que admiten zonas de Wavelength, consulte Zonas de Wavelength disponibles en la Guía para desarrolladores de AWS Wavelength.

Contenido

Describir las zonas de Wavelength

Puede usar la consola de Amazon EC2 o la interfaz de línea de comandos para determinar las zonas de Wavelength que están disponibles para su cuenta. Para obtener más información acerca de estas interfaces de línea de comandos, consulte Acceder a Amazon EC2.

Para encontrar las zonas de Wavelength mediante la consola

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

2. En la barra de navegación, seleccione el selector Regiones y, a continuación, seleccione la región.
3. En el panel de navegación, elija Panel de EC2.
4. En la esquina superior derecha de la página, elija Atributos de cuenta, Zonas.

Para encontrar las zonas de Wavelength mediante la AWS CLI

- Utilice el comando describe-availability-zones, tal y como se muestra a continuación, para describir las zonas de Wavelength dentro de la región especificada que están habilitadas para su cuenta.

```
aws ec2 describe-availability-zones --region region-name
```

- Utilice el comando describe-availability-zones como se muestra a continuación, para describir las zonas de Wavelength con independencia del estado de inscripción.

```
aws ec2 describe-availability-zones --all-availability-zones
```

Habilitar zonas de Wavelength

Antes de especificar una zona de Wavelength para un recurso o servicio, debe optar por zonas de Wavelength.

Consideraciones

- Algunos recursos de AWS no están disponibles en todas las regiones. Asegúrese de que puede crear los recursos que necesita en la región o zona de Wavelength deseada antes de iniciar una instancia en una zona de Wavelength específica.

Para darse de alta en la zona de Wavelength mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la esquina superior izquierda de la página, seleccione Nueva experiencia de EC2. No puede completar esta tarea utilizando la experiencia de consola anterior.
3. En la barra de navegación, seleccione el selector Regions y, a continuación, seleccione la región.
4. En el panel de navegación, elija Panel de EC2.

5. En la esquina superior derecha de la página, elija Atributos de cuenta, Zonas.
6. Elija una zona de Wavelength y seleccione Acción > Administrar grupo de zonas.
7. En Estado de suscripción, elija Habilitado.
8. Elija Actualizar.

Para habilitar las zonas de Wavelength mediante la AWS CLI

Utilice el comando modify-availability-zone-group.

Iniciar instancias en una zona de Wavelength

Al iniciar una instancia, puede especificar una subred que se encuentra en una zona de Wavelength. También asigna una dirección IP de operador de un grupo de perímetros de red, que es un conjunto único de zonas de disponibilidad, Local Zones o zonas de Wavelength desde las que AWS anuncia direcciones IP, por ejemplo, `us-east-1-wl1-bos-wlz-1`.

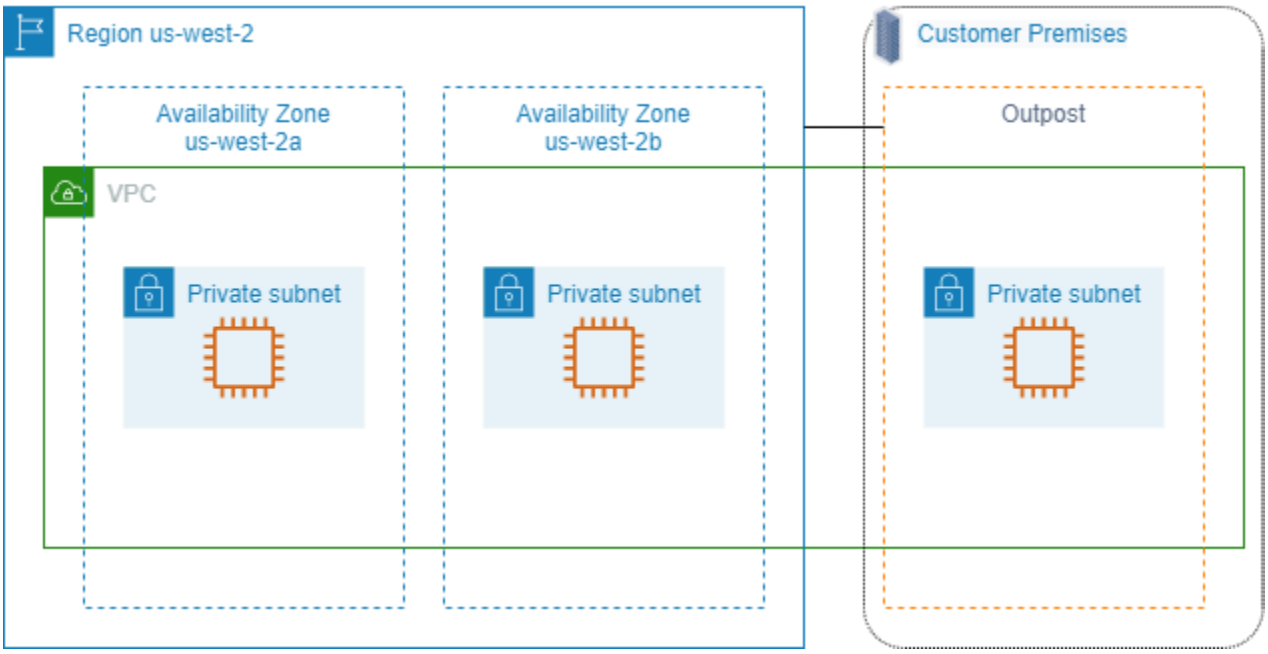
Para obtener información sobre cómo iniciar una instancia en una zona de Wavelength, consulte Introducción a AWS Wavelength en la Guía para desarrolladores de AWS Wavelength.

AWS Outposts

AWS Outposts es un servicio completamente administrado que extiende la infraestructura, los servicios, las API y las herramientas de AWS a las instalaciones del cliente. Al proporcionar acceso local a la infraestructura administrada de AWS, AWS Outposts habilita a los clientes a crear y ejecutar aplicaciones en las instalaciones mediante el uso de las mismas interfaces de programación que en las regiones de AWS, al mismo tiempo que utilizan recursos informáticos y de almacenamiento locales para reducir la latencia y las necesidades de procesamiento de datos locales.

Un Outpost es un grupo de capacidad informática y de almacenamiento de AWS implementada en un sitio del cliente. AWS opera, supervisa y administra esta capacidad como parte de una región de AWS. Puede crear subredes en el Outpost y especificarlas cuando cree recursos de AWS. Las instancias en las subredes de Outpost se comunican con otras instancias en la región de AWS mediante el uso de direcciones IP privadas, todo dentro de la misma VPC.

En el siguiente diagrama, se ilustran la región `us-west-2` de AWS, dos de sus zonas de disponibilidad y un Outpost. La VPC abarca las zonas de disponibilidad y el Outpost. El Outpost se encuentra en las instalaciones de un centro de datos del cliente. Cada zona de la VPC tiene una subred y cada subred tiene una instancia.



Para empezar a usar AWS Outposts, debe crear una instancia de Outpost y solicitar capacidad de Outpost. Para obtener más información acerca de las configuraciones de Outposts, consulte nuestro catálogo. Una vez que esté instalado el equipo del Outpost, la capacidad de computación y de almacenamiento estarán disponibles cuando se lancen instancias de Amazon EC2 en el Outpost.

Iniciar instancias en un Outpost

Puede iniciar instancias de EC2 en la subred de Outpost que ha creado. Los grupos de seguridad controlan el tráfico de entrada y salida de las instancias con interfaces de red elásticas de una subred de Outpost, igual que hacen para las instancias de una subred de zona de disponibilidad. Para conectarse a una instancia de EC2 en una subred de Outpost, puede especificar un par de claves al iniciar la instancia, como ocurre con las instancias de una subred de zona de disponibilidad.

Se recomienda limitar el volumen raíz de una instancia de un bastidor de Outpost a 30 GiB o menos. Puede especificar volúmenes de datos en la asignación de dispositivos de bloques de la AMI o la instancia para proporcionar almacenamiento adicional. Para recortar los bloques no utilizados del volumen raíz, consulte Cómo crear volúmenes de EBS dispersos en el blog de la red de socios de AWS.

Se recomienda aumentar el tiempo de espera de NVMe para el volumen raíz. Para obtener más información, consulte Tiempo de espera de las operaciones de E/S.

Para obtener información acerca de cómo crear un Outpost, consulte Introducción a AWS Outposts en la Guía del usuario de AWS Outposts.

Crear un volumen en un bastidor de Outpost

AWS Outposts ofrece factores de forma de bastidor y servidor. Si la capacidad está en un bastidor de Outpost, se pueden crear volúmenes de EBS en la subred de Outpost que se haya creado. Al crear el volumen, especifique el nombre de recurso de Amazon (ARN) del Outpost.

El siguiente comando create-volume crea un volumen vacío de 50 GB en el Outpost especificado.

```
aws ec2 create-volume --availability-zone us-east-2a --outpost-arn arn:aws:outposts:us-east-2:123456789012:outpost/op-03e6fecad652a6138 --size 50
```

Puede modificar dinámicamente el tamaño de los Amazon EBS volúmenes de gp2 sin desvincularlos. Para obtener más información acerca de cómo modificar un volumen sin desvincularlo, consulte Solicitar modificaciones a los volúmenes de EBS.

Direccionamiento IP de instancias Amazon EC2

Tanto Amazon EC2 como Amazon VPC admiten los protocolos de direcciones IPv4 e IPv6. De forma predeterminada, Amazon VPC utiliza el protocolo de direcciones IPv4 y este comportamiento no se puede desactivar. Cuando crea una VPC, debe especificar un bloque de CIDR IPv4 (un intervalo de direcciones IPv4 privadas). De manera opcional, puede asignar un bloque de CIDR IPv6 a su VPC y asignar direcciones IPv6 de dicho bloque a instancias de las subredes.

Contenido

- Direcciones de enlace local

Direcciones IPv4 privadas

Una dirección IPv4 privada es una dirección IP a la que no se puede obtener acceso desde Internet. Las direcciones IPv4 privadas se usan para la comunicación entre las instancias de una misma VPC. Para obtener más información acerca de los estándares y las especificaciones de las direcciones IPv4 privadas, consulte RFC 1918. Asignamos direcciones IPv4 privadas a las instancias mediante DHCP.

> **Note**
>
> Puede crear una VPC con un bloque de CIDR direccionable públicamente externo a los intervalos de direcciones IPv4 privadas especificadas en RFC 1918. Sin embargo, para esta documentación, las direcciones IP privadas IPv4 (o "direcciones IP privadas") son aquellas que se encuentran en el intervalo de CIDR IPv4 de su VPC.

Las subredes de VPC pueden ser de uno de los siguientes tipos:

Las subredes de VPC pueden ser de uno de los siguientes tipos:

- Subredes solo IPv4: solo puede crear recursos en estas subredes con direcciones IPv4 asignadas a ellas.
- Subredes solo IPv6: solo puede crear recursos en estas subredes con direcciones IPv6 asignadas a ellas.
- Subredes IPv4 e IPv6: puede crear recursos en estas subredes con direcciones IPv4 o IPv6 asignadas a ellas.

Al iniciar una instancia de EC2 en una subred de solo IPv4 o de doble pila (IPv4 e IPv6), la instancia recibe una dirección IP privada principal del rango de direcciones IPv4 de la subred. Para obtener más información, consulte dirección IP en la Guía del usuario de Amazon VPC. Si no especifica ninguna dirección IP privada principal al iniciar la instancia, se seleccionará una dirección IP disponible en el intervalo IPv4 de la subred en su nombre. Todas las instancias tienen una interfaz de red predeterminada (eth0) a la que se asigna la dirección IPv4 privada principal. También es posible especificar direcciones IPv4 privadas adicionales, conocidas como direcciones IPv4 privadas secundarias. A diferencia de las direcciones IP privadas principales, es posible volver a asignar

direcciones IP privadas secundarias de una instancia a otra. Para obtener más información, consulte Varias direcciones IP para sus instancias EC2.

Una dirección IPv4 privada, independientemente de si es una dirección principal o secundaria, permanece asociada a la interfaz de red cuando se detiene y reinicia o se hiberna y se reinicia la instancia, y se libera cuando termina la instancia.

Direcciones IPv4 públicas

Una dirección IP pública es una dirección IPv4 a la que se puede tener acceso desde Internet. Las direcciones públicas se usan para la comunicación entre sus instancias e Internet.

Cuando se inicia una instancia en una VPC predeterminada, recibe una dirección IP pública de forma predeterminada. Cuando se inicia una instancia en una VPC no predeterminada, la subred tiene un atributo que determina si las instancias iniciadas en esa subred reciben una dirección IP pública del grupo de direcciones IPv4 públicas. De forma predeterminada, las instancias iniciadas en una subred no predeterminada no reciben ninguna dirección IP pública.

Para controlar si una instancia recibe una dirección IP pública como se indica a continuación:

- Modifique el atributo de direcciones IP públicas de su subred. Para obtener más información, consulte Modificación del atributo de direcciones IPv4 públicas de su subred en la Guía del usuario de Amazon VPC.
- Habilite o deshabilite la característica de direcciones IP públicas durante la inicialización. Esta acción anulará el atributo de direcciones IP públicas de su subred. Para obtener más información, consulte Asignar una dirección IPv4 pública durante la inicialización de la instancia.
- Para anular la asignación de una dirección IP pública de la instancia tras iniciarla, administre las direcciones IP asociadas a una interfaz de red.

La dirección IP pública se asigna a su instancia de entre el grupo de direcciones IPv4 públicas de Amazon y no se asocia con su cuenta de AWS. Cuando se desvincula una dirección IP pública de su instancia, esta se libera de nuevo al grupo de direcciones IPv4 públicas y usted deja de poderlas utilizar.

En casos determinados, se libera la dirección IP pública desde su instancia o se asigna una dirección nueva:

- La dirección IP pública de una instancia se libera cuando esta se detiene, se hiberna o se termina. La instancia detenida o hibernada recibe una nueva dirección IP pública cuando se inicia.

- Liberaremos la dirección IP pública de la instancia si asocia una dirección IP elástica a su instancia. Cuando desvincula la dirección IP elástica de su instancia, esta recibe una dirección IP pública nueva.
- Si se ha liberado la dirección IP pública de la instancia en una VPC, la instancia no recibirá otra dirección IP pública nueva si hay más de una interfaz de red conectada a la instancia.
- Si la dirección IP pública de una instancia se libera mientras tiene una dirección IP privada secundaria asociada a una dirección IP elástica, la instancia no recibe una nueva dirección IP pública.

Si necesita una dirección IP pública persistente que se pueda asociar a instancias o desde instancias según sus necesidades, utilice una dirección IP elástica.

Si utiliza un DNS dinámico para asignar un nombre de DNS ya existente a la dirección IP pública de una instancia nueva, es posible que la dirección IP tarde hasta 24 horas en propagarse por Internet. A consecuencia de ello, es posible que las instancias nuevas no reciban tráfico, mientras que las instancias terminadas sigan recibiendo solicitudes. Para solucionar este problema, use una dirección IP elástica. Puede asignar su propia dirección IP elástica y asociarla a su instancia. Para obtener más información, consulte Direcciones IP elásticas.

> **Note**
>
> - AWS cobra por todas las direcciones IPv4 públicas, incluidas las direcciones IPv4 públicas asociadas a las instancias en ejecución y las direcciones IP elásticas. Para obtener más información, consulte la pestaña Dirección IPv4 pública en la página Precios de Amazon VPC.
> - Las instancias que obtienen acceso a otras instancias a través de sus direcciones IP de NAT públicas pagan por transferencias de datos regionales o de Internet, en función de si las instancias se encuentran en la misma región.

Optimización de las direcciones IPv4 públicas

AWS cobra por todas las direcciones IPv4 públicas, incluidas las direcciones IPv4 públicas asociadas a las instancias en ejecución y las direcciones IP elásticas. Para obtener más información, consulte la pestaña Dirección IPv4 pública en la página Precios de Amazon VPC.

La siguiente lista contiene las medidas que puede tomar para optimizar la cantidad de direcciones IPv4 públicas que utiliza:

- Use un equilibrador de carga elástico para equilibrar la carga del tráfico a sus instancias de EC2 y desactive la opción Asignar IP pública automáticamente en la ENI principal asignada a las instancias. Los equilibradores de carga usan una dirección IPv4 pública única, por lo que se reduce la cantidad de direcciones IPv4 públicas. También le recomendamos consolidar los equilibradores de carga existentes para reducir aún más el número de direcciones IPv4 públicas.
- Si el único motivo para utilizar una puerta de enlace NAT es utilizar SSH en una instancia de EC2 de una subred privada por motivos de mantenimiento o de emergencia, considere la posibilidad de utilizar el punto de conexión a instancia de EC2 en su lugar. Con el punto de conexión a instancia de EC2, puede conectarse a una instancia por Internet sin necesidad de que la instancia tenga una dirección IPv4 pública.
- Si sus instancias de EC2 se encuentran en una subred pública con direcciones IP públicas asignadas, considere trasladar las instancias a una subred privada, eliminar las direcciones IP públicas y utilizar una puerta de enlace NAT pública para permitir el acceso a las instancias de EC2 y desde estas. Tenga en cuenta que el uso de puertas de enlace NAT conlleva un costo. Utilice este método de cálculo para decidir si las puertas de enlace NAT son redituables. Para obtener el `Number of public IPv4 addresses` necesario para este cálculo, cree un informe de facturación, costos y uso de AWS.

  ```
  NAT gateway per hour + NAT gateway public IPs + NAT gateway transfer / Existing
   public IP cost
  ```

  Donde:

  - `NAT gateway per hour = $0.045 * 730 hours in a month * Number of Availability Zones the NAT gateways are in`
  - `NAT gateway public IPs = $0.005 * 730 hours in a month * Number of IPs associated with your NAT gateways`
  - `NAT gateway transfer = $0.045 * Number of GBs that will go through the NAT gateway in a month`
  - `Existing public IP cost = $0.005 * 730 hours in a month * Number of public IPv4 addresses`

  Si el total es inferior a 1, las puertas de enlace NAT son más baratas que las direcciones IPv4 públicas.

- Use AWS PrivateLink para conectarse de forma privada a los servicios de AWS o a servicios alojados en otras cuentas de AWS, en lugar de utilizar direcciones IPv4 públicas y puertas de enlace de Internet.
- Incorpore su propio rango de direcciones IP (BYOIP) en AWS y úselo para las direcciones IPv4 públicas en lugar de usar direcciones IPv4 públicas propiedad de Amazon.
- Desactive la opción de asignación automática de direcciones IPv4 públicas para las instancias iniciadas en subredes. Esta opción suele estar desactivada de forma predeterminada para las VPC cuando crea una subred, pero debe comprobar las subredes existentes para asegurarse de que esté desactivada.
- Si tiene instancias EC2 que no necesitan direcciones IPv4 públicas, compruebe que las interfaces de red conectadas a sus instancias tengan desactivada la opción Asignar IP pública automáticamente.
- Configure los puntos de conexión aceleradores en AWS Global Accelerator para las instancias de EC2 que estén en subredes privadas a fin de permitir que el tráfico de Internet fluya directamente hacia los puntos de conexión de sus VPC sin requerir direcciones IP públicas. También puede incorporar sus propias direcciones en AWS Global Accelerator y usar sus propias direcciones IPv4 para las direcciones IP estáticas de su acelerador.

Direcciones IP elásticas (IPv4)

Una dirección IP elástica es una dirección IPv4 pública que puede asignar a su cuenta. Puede asociarlo y desasociarlo de instancias según lo requiera. Se asigna a la cuenta hasta que elija liberarla. Para obtener información acerca de las direcciones IP elásticas y cómo usarlas, consulte Direcciones IP elásticas.

No se admiten las direcciones IP elásticas en IPv6.

Direcciones IPv6

Opcionalmente, puede asociar un bloque de CIDR IPv6 a su VPC y asociar bloques CIDR IPv6 a las subredes. El bloque de CIDR IPv6 de su VPC se asigna automáticamente de entre el grupo de direcciones IPv6 de Amazon; no puede elegir usted mismo el intervalo. Para obtener más información, consulte los siguientes temas en la Guía del usuario de Amazon VPC.

- Direccionamiento IP para sus VPC y subredes
- Agregue un bloque CIDR de IPv6 a su VPC

- Agregue un bloque CIDR de IPv6 a su subred

Las direcciones de IPv6 son únicas a nivel global y se pueden configurar para que sigan siendo privadas o para que estén disponibles en Internet. Su instancia recibirá una dirección IPv6 si hay un bloque de CIDR IPv6 asociado a la VPC y la subred, y si se cumple alguna de las condiciones siguientes:

- La subred está configurada para asignar automáticamente una dirección IPv6 a una instancia durante la inicialización. Para obtener más información, consulte Modificar el atributo de direcciones IPv6 de su subred.
- Asigna una dirección IPv6 a su instancia durante la inicialización.
- Asigna una dirección IPv6 a la interfaz de red principal de su instancia después de la inicialización.
- Asigna una dirección IPv6 a una interfaz de red de la misma subred y conecta la interfaz de red a la instancia tras la inicialización.

Cuando su instancia recibe una dirección IPv6 durante la inicialización, la dirección se asocia a la interfaz de red principal (eth0) de la instancia. Puede administrar direcciones IPv6 para la interfaz de red principal (eth0) para la instancia de las siguientes maneras:

- Asignación y anulación de la asignación de una dirección IPv6 a una interfaz de red. El número de direcciones IPv6 que puede asignar a una interfaz de red, así como el número de interfaces de red que puede conectar a una instancia varía según el tipo de instancia. Para obtener más información, consulte Direcciones IP por interfaz de red por tipo de instancia.
- Habilite una dirección IPv6 principal. La asignación de una dirección IPv6 principal le permite evitar interrumpir el tráfico a las instancias o ENI. Para obtener más información, consulte Crear una interfaz de red o Administrar direcciones IP.

Tenga en cuenta que la dirección IPv6 persiste al detener e iniciar, o hibernar e iniciar la instancia. Asimismo, se libera al terminar la instancia. No puede volver a asignar la dirección IPv6 mientras esté asignada a otra interfaz de red. Primero debe desasignarla.

Es posible controlar si las instancias están disponibles a través de sus direcciones IPv6 controlando el direccionamiento de su subred, o bien utilizando un grupo de seguridad y reglas de ACL de red. Para obtener más información, consulte Privacidad del tráfico entre redes en la Guía de usuario de Amazon VPC.

Para obtener más información acerca de los rangos de direcciones IPv6 reservados, consulte IANA IPv6 Special-Purpose Address Registry y RFC4291.

Trabajar con las direcciones IPv4 de las instancias

Puede asignar una dirección IPv4 pública a su instancia cuando la lance. Puede ver las direcciones IPv4 de su instancia en la consola a través de la página Instancias o la página Interfaces de red.

Contenido

Ver las direcciones IPv4

Puede utilizar la consola de Amazon EC2 para ver las direcciones IPv4 públicas y privadas de sus instancias. También puede determinar las direcciones IPv4 públicas e IPv4 privadas de su instancia desde la misma instancia mediante metadatos de esta. Para obtener más información, consulte Trabajar con metadatos de instancias.

La dirección IPv4 pública se muestra como propiedad de la interfaz de red en la consola, aunque se asigna a la dirección IPv4 privada principal mediante NAT. Por lo tanto, si consulta las propiedades de su interfaz de red en su instancia como, por ejemplo, mediante `ifconfig` (Linux) o `ipconfig` (Windows), verá que no se muestra la dirección IPv4 pública. Para determinar la dirección IPv4 pública de la instancia a partir de una instancia, utilice los metadatos de la instancia.

Para ver las direcciones IPv4 de una instancia 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 Acceder a Amazon EC2.

- describe-instances (AWS CLI)
- Get-EC2InstanceAWS Tools for Windows PowerShell

Para determinar las direcciones IPv4 de su instancia mediante metadatos de la instancia

1. Conéctese a la instancia. Para obtener más información, consulte Conexión con instancias EC2.
2. Utilice el siguiente comando para obtener acceso a la dirección IP privada.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
 "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
meta-data/local-ipv4
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/local-ipv4
```

Tools for Windows PowerShell

```
PS C:\> Invoke-RestMethod http://169.254.169.254/latest/meta-data/local-ipv4
```

3. Utilice el siguiente comando para obtener acceso a la dirección IP pública. Si hay una dirección IP elástica asociada a la instancia, el valor devuelto será el de dicha dirección.

   IMDSv2

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
    "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   meta-data/public-ipv4
   ```

   IMDSv1

   ```
   [ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-ipv4
   ```

   Tools for Windows PowerShell

   ```
   PS C:\> Invoke-RestMethod http://169.254.169.254/latest/meta-data/public-ipv4
   ```

Asignar una dirección IPv4 pública durante la inicialización de la instancia

Todas las subredes tienen un atributo que determina si se asigna una dirección IP pública a las instancias iniciadas en dichas subredes. De forma predeterminada, las subredes no predeterminadas

tienen este atributo configurado como false, mientras que todas las subredes predeterminadas tienen este atributo configurado como true. Cuando inicia una instancia, también tiene a su disposición una característica de dirección IPv4 pública para que pueda controlar si se asigna a su instancia una dirección IPv4 pública; puede anular el comportamiento predeterminado del atributo de dirección IP de la subred. La dirección IPv4 pública se asigna de entre el grupo de direcciones IPv4 públicas de Amazon; se asigna a la interfaz de red con el índice de dispositivo eth0. Esta característica depende de determinadas condiciones que se puedan dar en el momento en que se inicia la instancia.

Consideraciones

- Para anular la asignación de la dirección IP pública desde la instancia tras iniciarla, administre las direcciones IP asociadas a una interfaz de red. Para obtener más información acerca de las direcciones IPv4 públicas, consulte Direcciones IPv4 públicas.
- No puede asignar automáticamente una dirección IP pública si especifica más de una interfaz de red. Además, no puede anular la configuración de la subred con la característica de asignación automática de IP pública si especifica una interfaz de red existente para eth0.
- Independientemente de si asigna una dirección IP pública a su instancia durante la inicialización o no, puede asociar una dirección IP elástica a su instancia luego de iniciarla. Para obtener más información, consulte Direcciones IP elásticas. También puede modificar el comportamiento de las direcciones IPv4 públicas de su subred. Para obtener más información, consulte Modificación del atributo de direcciones IPv4 públicas de su subred.

Para asignar una dirección IPv4 pública durante la inicialización de la instancia con la consola

Siga el procedimiento para iniciar una instancia y, cuando defina la configuración en Configuración de red, elija la opción Asignar automáticamente IP pública.

Para habilitar o deshabilitar la característica de direcciones IP públicas 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 Acceder a Amazon EC2.

- Utilice la opción `--associate-public-ip-address` o `--no-associate-public-ip-address` con el comando run-instances (AWS CLI)
- Utilice el parámetro `-AssociatePublicIp` con el comando New-EC2Instance (AWS Tools for Windows PowerShell)

Trabajar con las direcciones IPv6 de las instancias

Puede ver las direcciones IPv6 asignadas a la instancia, asignar una dirección IPv6 pública a la instancia o anular la asignación de una dirección IPv6 de la instancia. Puede ver estas direcciones en la consola a través de la página Instancias o la página Interfaces de red.

Contenido

Ver las direcciones IPv6

Puede utilizar la consola de Amazon EC2, la AWS CLI y los metadatos de la instancia para ver las direcciones IPv6 de las instancias.

Para ver las direcciones IPv6 de una instancia mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instancias.
3. Seleccione la instancia.
4. En la pestaña Redes, localice Direcciones IPv6.

Para ver las direcciones IPv6 de una instancia 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 Acceder a Amazon EC2.

- describe-instances (AWS CLI)
- Get-EC2InstanceAWS Tools for Windows PowerShell

Para ver las direcciones IPv6 de una instancia mediante metadatos de instancia

1. Conéctese a la instancia. Para obtener más información, consulte Conexión con instancias EC2.
2. Obtenga la dirección MAC de la instancia de `http://169.254.169.254/latest/meta-data/network/interfaces/macs/`.

3. Utilice el siguiente comando para visualizar la dirección IPv6.

   IMDSv2

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
    "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   meta-data/network/interfaces/macs/mac-address/ipv6s
   ```

   IMDSv1

   ```
   [ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/network/interfaces/
   macs/mac-address/ipv6s
   ```

   Tools for Windows PowerShell

   ```
   PS C:\> Invoke-RestMethod http://169.254.169.254/latest/meta-data/network/
   interfaces/macs/mac-address/ipv6s
   ```

Asignar una dirección IPv6 a una instancia

Si su VPC y las subredes tienen bloques de CIDR IPv6 asociados, puede asignar una dirección IPv6 a su instancia durante la inicialización o después de este. La dirección IPv6 se asigna de entre el intervalo de direcciones IPv6 de la subred; se asigna a la interfaz de red con el índice de dispositivo eth0.

Para asignar una dirección IPv6 durante la inicialización de la instancia

Siga el procedimiento para iniciar una instancia y, cuando defina la configuración en Configuración de red, elija la opción Asignar automáticamente IP IPv6.

Para asignar una dirección IPv6 después de la inicialización

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instances (Instancias).
3. Seleccione su instancia y elija Acciones, Redes, Administrar direcciones IP.
4. Amplíe la interfaz de red. En Direcciones IP IPv6, elija Asignar nueva dirección IP. Escriba una dirección IPv6 del rango de la subred o deje el campo en blanco para permitir que Amazon elija una dirección IPv6 automáticamente.

5. Seleccione Guardar.

Para asignar una dirección IPv6 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 Acceder a Amazon EC2.

- Utilice la opción `--ipv6-addresses` con el comando run-instances (AWS CLI).
- Utilice la propiedad `Ipv6Addresses` de `-NetworkInterface` en el comando New-EC2Instance (AWS Tools for Windows PowerShell)
- assign-ipv6-addresses (AWS CLI)
- Register-EC2Ipv6AddressList (AWS Tools for Windows PowerShell)

Anular la asignación de una dirección IPv6 de una instancia

Puede anular la asignación de una dirección IPv6 de una instancia en cualquier momento.

Para anular la asignación de una dirección IPv6 de una instancia con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instances (Instancias).
3. Seleccione su instancia y elija Acciones, Redes, Administrar direcciones IP.
4. Amplíe la interfaz de red. En Direcciones IPv6, elija Desasignar junto a la dirección IPv6.
5. Seleccione Guardar.

Para anular la asignación de una dirección IPv6 de una instancia 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 Acceder a Amazon EC2.

- unassign-ipv6-addresses (AWS CLI)
- Unregister-EC2Ipv6AddressList (AWS Tools for Windows PowerShell)

Varias direcciones IP para sus instancias EC2

Puede especificar varias direcciones IPv4 e IPv6 privadas para las instancias. El número de interfaces de red y de direcciones IPv4 e IPv6 privadas que puede especificar para una instancia depende del tipo de instancia. Para obtener más información, consulte Direcciones IP por interfaz de red por tipo de instancia.

Puede ser útil asignar varias direcciones IP a una instancia en su VPC para hacer lo siguiente:

- Alojar varios sitios web en un único servidor utilizando varios certificados SSL en un único servidor y asociando cada certificado a una dirección IP específica.
- Tratar dispositivos de red, como firewalls o balanceadores de carga, que tienen varias direcciones IP para cada interfaz de red.
- Redirigir el tráfico interno a una instancia en espera en el caso de que su instancia dé un error, reasignando la dirección IP secundaria a la instancia en espera.

Contenido

Cómo funcionan varias direcciones IP

En la lista siguiente se explica cómo varias direcciones IP funcionan con interfaces de red:

- Puede asignar una dirección IPv4 privada secundaria a cualquier interfaz de red.
- Puede asignar varias direcciones IPv6 a una interfaz de red que esté en una subred que tenga un bloque de CIDR IPv6 asociado.
- Debe elegir una dirección IPv4 secundaria de entre el intervalo del bloque de CIDR IPv4 de la subred para la interfaz de red.
- Debe elegir las direcciones IPv6 de entre el intervalo del bloque de CIDR IPv6 de la subred para la interfaz de red.
- Asocie los grupos de seguridad con las interfaces de red, no con direcciones IP individuales. Por lo tanto, cada dirección IP que especifique en una interfaz de red estará sujeta al grupo de seguridad de su interfaz de red.

- Se pueden asignar varias direcciones IP a interfaces de red adjuntadas a instancias en ejecución o detenidas, y también se puede anular su asignación.
- Las direcciones IPv4 privadas secundarias asignadas a una interfaz de red se pueden volver a asignar a otra instancia si usted lo permite explícitamente.
- Una dirección IPv6 no se puede volver a asignar a otra interfaz de red; primero debe anular la asignación de la dirección IPv6 de la interfaz de red existente.
- Si asigna varias direcciones IP a una interfaz de red mediante las herramientas de línea de comandos o la API, toda la operación fracasará si una de las direcciones IP no se puede asignar.
- Las direcciones IPv4 privadas principales y secundarias, las direcciones IP elásticas y las direcciones IPv6 se quedarán en la interfaz de red cuando esta se desconecte de una instancia o cuando se conecte a otra instancia.
- Aunque no puede desconectar la interfaz de red principal desde una instancia, puede volver a asignar la dirección IPv4 privada secundaria de la interfaz de red principal a otra interfaz de red.

En la lista siguiente se explica cómo funcionan varias direcciones IP con direcciones IP elásticas (solo IPv4):

- Todas las direcciones IPv4 privadas se pueden asociar a una dirección IP elástica única y viceversa.
- Cuando se vuelve a asignar una dirección IPv4 privada secundaria a otra interfaz, la dirección IPv4 privada secundaria conserva su asociación con la dirección IP elástica.
- Cuando se anula la asignación de una dirección IPv4 privada secundaria de una interfaz, automáticamente se anula la asociación de una dirección IP elástica asociada de la dirección IPv4 privada secundaria.

Trabajar con varias direcciones IPv4

Puede asignar una dirección IPv4 privada secundaria a una instancia, asociar una dirección IPv4 elástica a una dirección IPv4 privada secundaria y anular la asignación de una dirección IPv4 privada secundaria.

Tareas

- Asignar una dirección IPv4 privada secundaria
- Configuración del sistema operativo para reconocer direcciones IPv4 privadas secundarias

- Asociar una dirección IP elástica con la dirección IPv4 privada secundaria
- Ver las direcciones IPv4 privadas secundarias
- Anular la asignación de una dirección IPv4 privada secundaria

Asignar una dirección IPv4 privada secundaria

Puede asignar la dirección IPv4 privada secundaria a la interfaz de red para una instancia cuando inicia la instancia o después de esta esté ejecutándose.

Para asignar una dirección IPv4 privada secundaria al iniciar una instancia

1. Siga el procedimiento para Iniciar una instancia. En Configuración de red, elija Editar.
2. Seleccione una VPC y una subred.
3. Expanda Configuración de red avanzada.
4. En IP secundaria, elija Asignar automáticamente e ingrese el número de direcciones IP (Amazon asigna automáticamente direcciones IPv4 secundarias) o elija Asignar manualmente e ingrese las direcciones IPv4.
5. Complete los pasos restantes para Iniciar la instancia.

Para asignar una dirección IPv4 secundaria durante la inicialización utilizando la línea de comandos

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

- La opción `--secondary-private-ip-addresses` con el comando run-instances (AWS CLI)
- Defina `-NetworkInterface` y especifique el parámetro `PrivateIpAddresses` con el comando New-EC2Instance (AWS Tools for Windows PowerShell).

Para asignar una dirección IPv4 privada secundaria a una interfaz de red

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Interfaces de red y, a continuación, seleccione la interfaz de red para la instancia.
3. Elija Acciones, Administrar direcciones IP.
4. Amplíe la interfaz de red. En Direcciones IPv4, elija Asignar nueva dirección IP.

5. Escriba una dirección IPv4 específica que esté dentro del intervalo de la subred para la instancia o deje el campo en blanco para que Amazon seleccione una dirección IPv4 en su lugar.
6. (Opcional) Seleccione Permitir para permitir que se vuelva a asignar la dirección IP privada secundaria si ya está asignada a otra interfaz de red.
7. Seleccione Guardar.

O bien, puede asignar una dirección IPv4 privada secundaria a una instancia. Elija Instancias en el panel de navegación, seleccione la instancia y, a continuación, elija Acciones, Redes y Administrar direcciones IP. Puede configurar la misma información que configuró en los pasos anteriores. La dirección IP se asigna a la interfaz de red principal (eth0) para la instancia.

Asignación de una dirección IPv4 privada secundaria a una instancia que ya existe 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 Acceder a Amazon EC2.

- assign-private-ip-addresses (AWS CLI)
- Register-EC2PrivateIpAddress (AWS Tools for Windows PowerShell)

Configuración del sistema operativo para reconocer direcciones IPv4 privadas secundarias

Después de asignar una dirección IPv4 privada secundaria a su instancia, tiene que configurar el sistema operativo en su instancia para reconocer la dirección IP privada secundaria.

instancias de Linux

- Si utiliza Amazon Linux, el paquete ec2-net-utils puede ejecutar este paso en su lugar. Configura las interfaces de red adicionales que adjunta mientras la instancia se ejecuta, actualiza las direcciones IPv4 secundarias durante la renovación de la concesión DHCP y actualiza las reglas de enrutamiento relacionadas. Puede actualizar inmediatamente la lista de interfaces ejecutando el comando `sudo service network restart` y viendo la lista actualizada utilizando `ip addr li`. Si necesita tener un control manual de la configuración de la red, puede eliminar el paquete ec2-net-utils. Para obtener más información, consulte Configure su interfaz de red mediante ec2-net-utils para Amazon Linux 2.
- Si utiliza otra distribución de Linux, consulte la documentación sobre la distribución de Linux. Busque información sobre cómo configurar interfaces de red adicionales y direcciones IPv4

secundarias. Si la instancia tiene dos o varias interfaces en la misma subred, busque información sobre cómo usar reglas de enrutamiento para evitar el enrutamiento asimétrico.

instancias de Windows

Para obtener más información, consulte Configurar una dirección IPv4 privada secundaria para instancias de Windows.

Asociar una dirección IP elástica con la dirección IPv4 privada secundaria

Para asociar una dirección IP elástica a una dirección IPv4 privada secundaria

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Direcciones IP elásticas.
3. Selección de la casilla de verificación de la dirección IP elástica
4. Elija Acciones y, a continuación, Asociar dirección IP elástica.
5. En Tipo de recurso, elija Interfaz de red. Seleccione la interfaz de red y, a continuación, seleccione la dirección IP secundaria en la lista Dirección IP privada.
6. En Interfaz de red, seleccione la interfaz de red. Seleccione la dirección IP secundaria en la lista Dirección IP privada.
7. En Dirección IP privada, seleccione la dirección IP secundaria.
8. Elija Asociar.

Para asociar una dirección IP elástica con una dirección IPv4 privada usando la línea de comandos

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

- associate-address (AWS CLI)
- Register-EC2Address (AWS Tools for Windows PowerShell)

Ver las direcciones IPv4 privadas secundarias

Para ver las direcciones IPv4 privadas asignadas a una interfaz de red

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Interfaces de red.

3. Seleccione la casilla de verificación de la interfaz de red.
4. En la pestaña Detalles, en Direcciones IP, busque Dirección IPv4 privada y Direcciones IPv4 privadas secundarias.

Para ver las direcciones IPv4 privadas asignadas a una instancia

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Seleccione la casilla de verificación de la instancia.
4. En la pestaña Redes, en Detalles de redes, busque Direcciones IPv4 privadas y Direcciones IPv4 privadas secundarias.

Anular la asignación de una dirección IPv4 privada secundaria

Si ya no necesita una dirección IPv4 privada secundaria, puede anular su asignación a la instancia o a la interfaz de red. Cuando se anula la asignación de una dirección IPv4 privada secundaria de una interfaz de red, también se anula la asociación de la dirección IP elástica (si existe).

Para anular la asignación de una dirección IPv4 privada secundaria de una instancia

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Seleccione una instancia y elija Acciones, Redes, Administrar direcciones IP.
4. Amplíe la interfaz de red. En Direcciones IPv4, elija Anular la asignación para la dirección IPv4 cuya asignación va a anular.
5. Seleccione Guardar.

Para anular la asignación de una dirección IPv4 privada secundaria de una interfaz de red.

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Network Interfaces.
3. Seleccione la interfaz de red y elija Acciones y Administrar direcciones IP.
4. Amplíe la interfaz de red. En Direcciones IPv4, elija Anular la asignación para la dirección IPv4 cuya asignación va a anular.
5. Seleccione Guardar.

Para eliminar la asignación de una dirección IPv4 privada secundaria utilizando la línea de comandos

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

- unassign-private-ip-addresses (AWS CLI)
- Unregister-EC2PrivateIpAddress (AWS Tools for Windows PowerShell)

Trabajar con varias direcciones IPv6

Puede asignar varias direcciones IPv6 a su instancia, ver las direcciones IPv6 asignadas a su instancia y anular la asignación de direcciones IPv6 de su instancia.

Contenido

- Asignar varias direcciones IPv6
- Ver sus direcciones IPv6
- Anular la asignación de una dirección IPv6

Asignar varias direcciones IPv6

Puede asignar una o varias direcciones IPv6 a su instancia durante la inicialización o después de este. Para asignar una dirección IPv6 a una instancia, la VPC y la subred en las que inicia la instancia deben tener un bloque de CIDR IPv6 asociado.

Para asignar varias direcciones IPv6 durante la inicialización

1. Siga el procedimiento para Iniciar una instancia. En Configuración de red, elija Editar.
2. Seleccione una VPC y una subred.
3. Expanda Configuración de red avanzada.
4. En IP IPv6, elija Asignar automáticamente y el número de direcciones IP (Amazon asigna automáticamente las direcciones IPv6) o elija Asignar manualmente e ingrese las direcciones IPv6.
5. Complete los pasos restantes para iniciar la instancia.

Puede utilizar la pantalla Instancias de la consola de Amazon EC2 para asignar varias direcciones IPv6 a una instancia existente. De esta forma, podrá asignar direcciones IPv6 a la interfaz de red

principal (eth0) para la instancia. Para asignar una dirección IPv6 específica a la instancia, asegúrese de que la dirección IPv6 no esté ya asignada a otra instancia o interfaz de red.

Para asignar varias direcciones IPv6 a una instancia ya existente

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Seleccione la instancia y elija Acciones, Redes y Administrar direcciones IP.
4. Amplíe la interfaz de red. En Direcciones IPv6, elija Asignar nueva dirección IP para cada dirección IPv6 que agregará. Puede especificar una dirección IPv6 del rango de la subred o dejar el campo vacío para que Amazon elija una dirección IPv6 en su lugar.
5. Seleccione Guardar.

De manera alternativa, puede asignar varias direcciones IPv6 a una interfaz de red ya existente. La interfaz de red debe haberse creado en una subred que tenga asociado un bloque de CIDR IPv6. Para asignar una dirección IPv6 específica a la interfaz de red, asegúrese de que la dirección no esté ya asignada a otra interfaz de red.

Para asignar varias direcciones IPv6 a una interfaz de red

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Network Interfaces.
3. Seleccione la interfaz de red y elija Acciones y Administrar direcciones IP.
4. Amplíe la interfaz de red. En Direcciones IPv6, elija Asignar nueva dirección IP para cada dirección IPv6 que agregará. Puede especificar una dirección IPv6 del rango de la subred o dejar el campo vacío para que Amazon elija una dirección IPv6 en su lugar.
5. Seleccione Guardar.

Información general de la CLI

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

- Asignación de una dirección IPv6 durante la inicialización:
  - Utilice las opciones `--ipv6-addresses` o `--ipv6-address-count` con el comando run-instances (AWS CLI)

  - Defina `-NetworkInterface` y especifique los parámetros `Ipv6Addresses` o `Ipv6AddressCount` con el comando New-EC2Instance (AWS Tools for Windows PowerShell).
- Asignación de una dirección IPv6 a una interfaz de red:
  - assign-ipv6-addresses (AWS CLI)
  - Register-EC2Ipv6AddressList (AWS Tools for Windows PowerShell)

Ver sus direcciones IPv6

Puede ver las direcciones IPv6 de una instancia o de una interfaz de red.

Para ver las direcciones IPv6 asignadas a una instancia

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Seleccione la casilla de verificación de su instancia.
4. En la pestaña Redes, busque el campo Direcciones IPv6.

Para ver las direcciones IPv6 asignadas a una interfaz de red

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Network Interfaces.
3. Seleccione la casilla de verificación de su interfaz de red.
4. En la pestaña Detalles, en Direcciones IP, busque el campo Direcciones IPv6.

Información general de la CLI

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

- Visualización de las direcciones IPv6 de una instancia:
  - describe-instances (AWS CLI)
  - Get-EC2InstanceAWS Tools for Windows PowerShell
- Visualización de las direcciones IPv6 de una interfaz de red:
  - describe-network-interfaces (AWS CLI)
  - Get-EC2NetworkInterface (AWS Tools for Windows PowerShell)

Anular la asignación de una dirección IPv6

Puede anular la asignación de una dirección IPv6 de la interfaz de red principal de una instancia o puede anular la asignación de una dirección IPv6 de una interfaz de red.

Para anular una dirección IPv6 de una instancia

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Seleccione la casilla de verificación de su instancia y elija Acciones, Redes y Administrar direcciones IP.
4. Amplíe la interfaz de red. En Direcciones IPv6, elija Desasignar junto a la dirección IPv6.
5. Seleccione Guardar.

Para anular la asignación de una dirección IPv6 de una interfaz de red

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Network Interfaces.
3. Seleccione la casilla de verificación de su instancia y elija Acciones y Administrar direcciones IP.
4. Amplíe la interfaz de red. En Direcciones IPv6, elija Desasignar junto a la dirección IPv6.
5. Seleccione Guardar.

Información general de la CLI

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

- unassign-ipv6-addresses (AWS CLI)
- Unregister-EC2Ipv6AddressList (AWS Tools for Windows PowerShell)

Configurar una dirección IPv4 privada secundaria para instancias de Windows

Puede especificar varias direcciones IPv4 privadas para las instancias. Después de asignar una dirección IPv4 privada secundaria a una instancia, debe configurar el sistema operativo en la instancia para que reconozca la dirección IPv4 privada secundaria.

> **Note**
>
> Estas instrucciones se basan en Windows Server 2022. La implementación de estos pasos puede variar según el sistema operativo de la instancia de Windows.

Tareas

- Requisitos previos
- Paso 1: Configurar una dirección IP estática en la instancia
- Paso 2: Configurar una dirección IP privada secundaria para la instancia
- Paso 3: Configurar las aplicaciones para que usen la dirección IP privada secundaria

Requisitos previos

1. Asigne la dirección IPv4 privada secundaria a la interfaz de red para la instancia. Puede asignar la dirección IPv4 privada secundaria cuando inicia la instancia o después de esta esté ejecutándose. Para obtener más información, consulte Asignar una dirección IPv4 privada secundaria.
2. Asigne una dirección IP elástica y asóciela a la dirección IPv4 privada secundaria. Para obtener más información, consulte Asignar una dirección IP elástica y Asociar una dirección IP elástica con la dirección IPv4 privada secundaria.

Paso 1: Configurar una dirección IP estática en la instancia

Para habilitar una instancia de Windows para que use varias direcciones IP, debe configurarla para usar direcciones IP estáticas en lugar de un servidor DHCP.

> **Important**
>
> Cuando configura una dirección IP estática en la instancia, la dirección IP debe coincidir exactamente con lo que se muestra en la consola, la CLI o la API. Si escribe estas direcciones IP de forma incorrecta, la instancia podría no ser alcanzable.

Para configurar direcciones IP estáticas en una instancia de Windows

1. Conéctese a la instancia.

2. Busque la dirección IP, la máscara de subred y las direcciones de puertas de enlace predeterminadas de la instancia siguiendo los pasos siguientes:

   - Ejecute el siguiente comando en PowerShell:

     ```
     ipconfig /all
     ```

     Examine el resultado que obtenga y anote los valores IPv4 Address (Dirección IPv4), Subnet Mask (Máscara de subred), Default Gateway (Puerta de enlace predeterminada) y DNS Servers (Servidores DNS) de la interfaz de red. El resultado debería parecerse al siguiente ejemplo:

     ```
     ...

     Ethernet adapter Ethernet 4:

        Connection-specific DNS Suffix  . : us-west-2.compute.internal
        Description . . . . . . . . . . . : Amazon Elastic Network Adapter #2
        Physical Address. . . . . . . . . : 02-9C-3B-FC-8E-67
        DHCP Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        Link-local IPv6 Address . . . . . : fe80::f4d1:a773:5afa:cd1%7(Preferred)
        IPv4 Address. . . . . . . . . . . : 10.200.0.128(Preferred)
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Lease Obtained. . . . . . . . . . : Monday, April 8, 2024 12:19:29 PM
        Lease Expires . . . . . . . . . . : Monday, April 8, 2024 4:49:30 PM
        Default Gateway . . . . . . . . . : 10.200.0.1
        DHCP Server . . . . . . . . . . . : 10.200.0.1
        DHCPv6 IAID . . . . . . . . . . . : 151166011
        DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2D-67-AC-FC-12-34-9A-BE-A5-
     E7
        DNS Servers . . . . . . . . . . . : 10.200.0.2
        NetBIOS over Tcpip. . . . . . . . : Enabled
     ```

3. Ejecute el siguiente comando en PowerShell para abrir el Centro de redes y recursos compartidos:

   ```
   & $env:SystemRoot\system32\control.exe ncpa.cpl
   ```

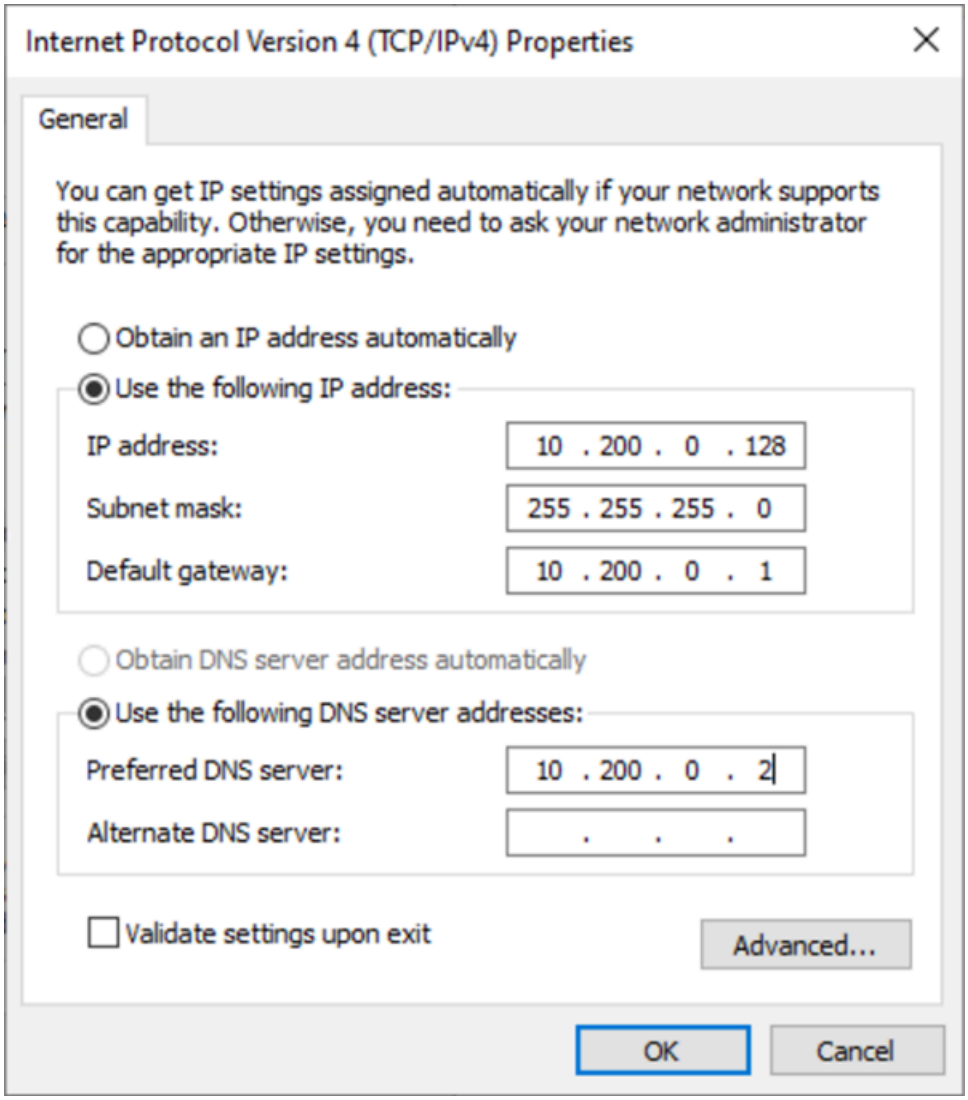
4. Abra el menú contextual (haga clic con el botón derecho) de la interfaz de red (conexión de área local o Ethernet) y elija Propiedades.

5. Elija Protocolo de Internet versión 4 (TCP/IPv4), Propiedades.
6. En el cuadro de diálogo Propiedades: Protocolo de Internet, versión 4 (TCP/IPv4), elija Usar la siguiente dirección IP, escriba los valores siguientes y elija Aceptar.

Campo	Valor
Dirección IP	La dirección IPv4 obtenida en el paso 2 anterior.
Máscara de subred	La máscara de subred obtenida en el paso 2 anterior.
Puerta de enlace predeterminada	La dirección predeterminada de la puerta de enlace obtenida en el paso 2 anterior.
Servidor DNS preferido	El servidor DNS obtenido en el paso 2 anterior.
Servidor DNS alternativo	El servidor DNS alternativo obtenido en el paso 2 anterior. Si el servidor DNS alternativo no figura en la lista, deje este campo en blanco.

Important

Si establece la dirección IP en un valor que no sea la dirección IP actual, perderá la conexión con la instancia.



Perderá la conexión RDP con la instancia de Windows durante unos segundos mientras la instancia pasa de usar DHCP a usar direcciones estáticas. La instancia retiene la misma información de la dirección IP que antes, pero ahora esta información es estática y no está administrada por DHCP.

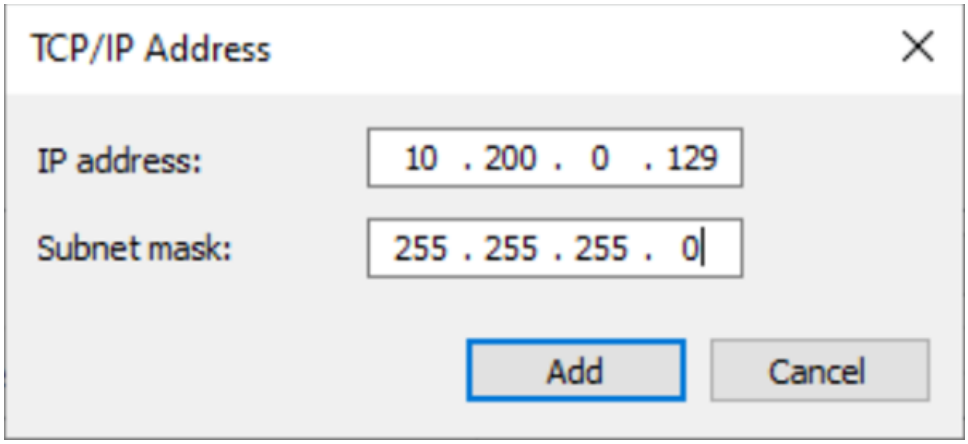
Paso 2: Configurar una dirección IP privada secundaria para la instancia

Una vez configurada la dirección IP estática en la instancia de Windows, puede pasar a preparar una segunda dirección IP privada.

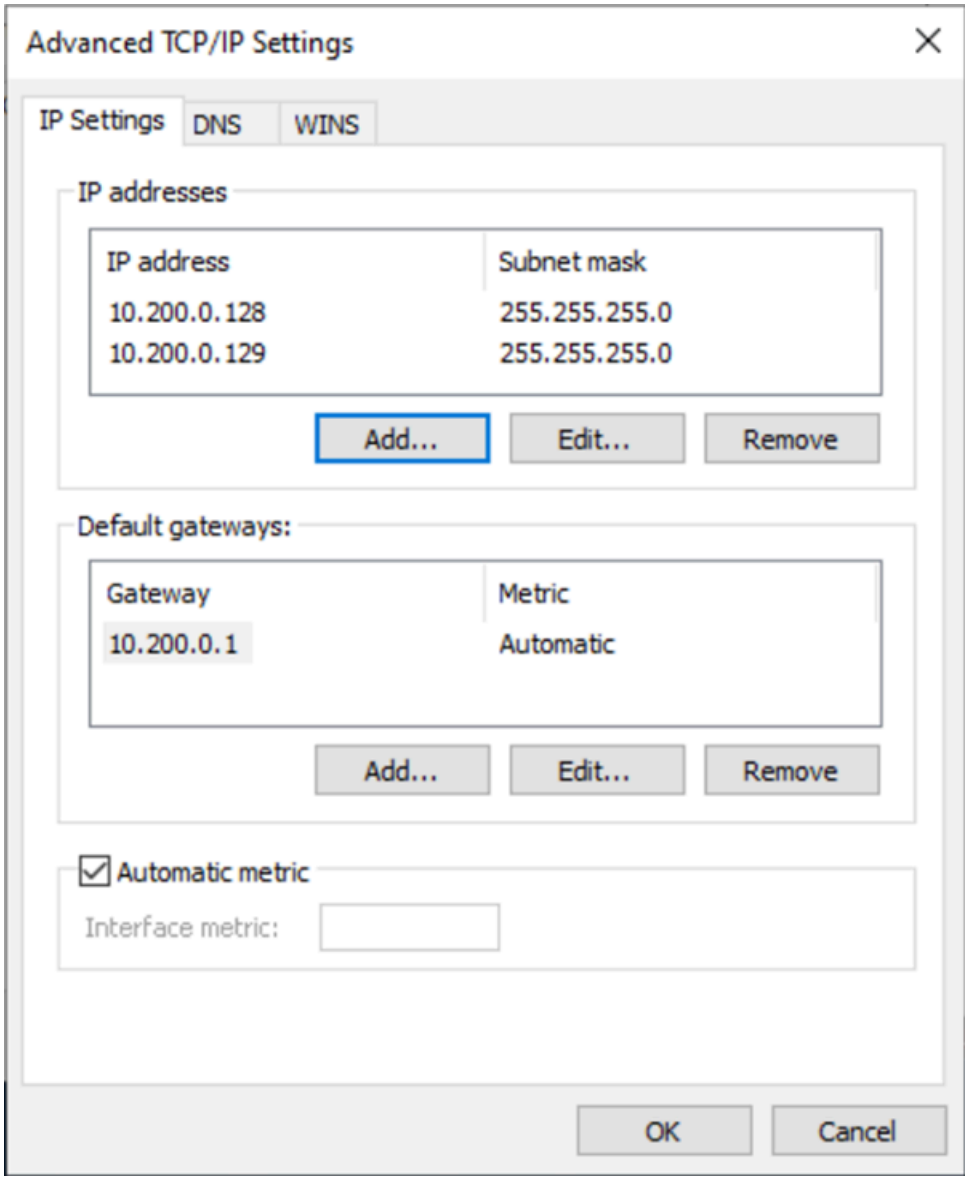
Para configurar una dirección IP secundaria

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

2. En el panel de navegación, elija Instances (Instancia[s]) y seleccione la instancia.
3. En Redes, anota la dirección IP secundaria.
4. Conéctese a la instancia.
5. En la instancia de Windows, elija Inicio, Panel de control.
6. Elija Redes e Internet, Centro de redes y recursos compartidos.
7. Seleccione la interfaz de red (conexión de área local o Ethernet) y elija Propiedades.
8. En la página Propiedades de Conexión de área local, elija Protocolo de Internet, versión 4 (TCP/IPv4), Propiedades, Opciones avanzadas.
9. Elija Add (Añadir).
10. En el cuadro de diálogo Dirección TCP/IP, escriba la dirección IP privada secundaria en Dirección IP. En Subnet mask (Máscara de subred), escriba la misma que escribió para la dirección IP privada principal en Paso 1: Configurar una dirección IP estática en la instancia y elija Add (Agregar).



11. Compruebe la configuración de la dirección IP y elija Aceptar.



12. Elija Aceptar, Cerrar.
13. Para confirmar la dirección IP secundaria que se ha añadido al sistema operativo, ejecute el comando `ipconfig /all` en PowerShell. El resultado debe tener el siguiente aspecto:

```
Ethernet adapter Ethernet 4:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Amazon Elastic Network Adapter #2
   Physical Address. . . . . . . . . : 02-9C-3B-FC-8E-67
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::f4d1:a773:5afa:cd1%7(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.200.0.128(Preferred)
```

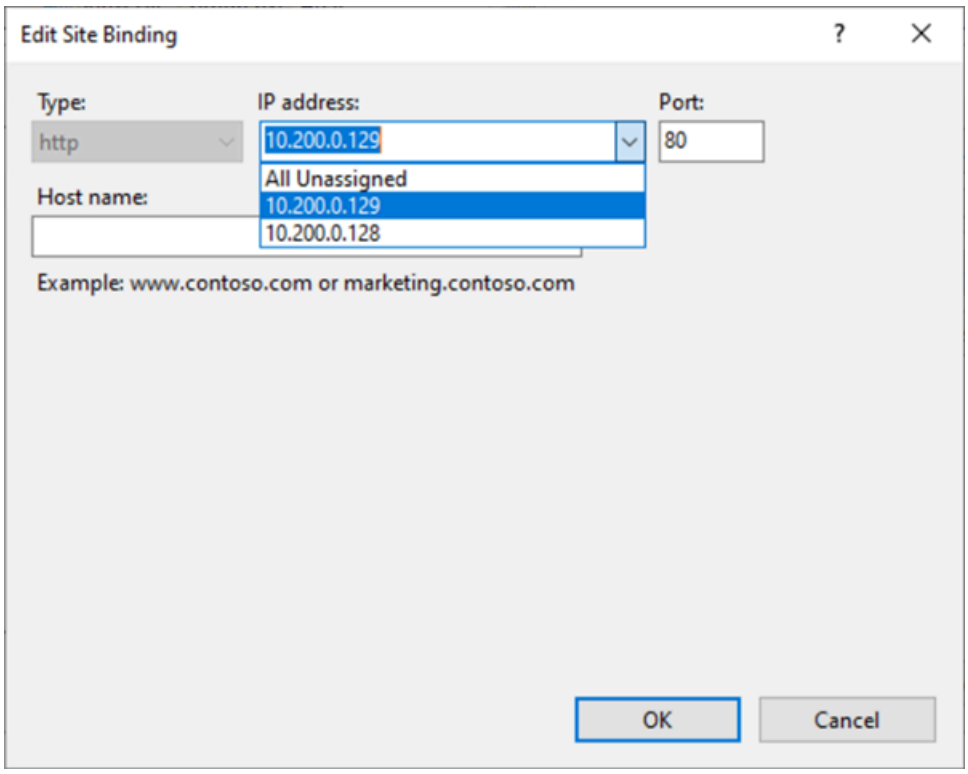
```
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   IPv4 Address. . . . . . . . . . . : 10.200.0.129(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.200.0.1
   DHCPv6 IAID . . . . . . . . . . . : 151166011
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2D-67-AC-FC-12-34-9A-BE-A5-E7
   DNS Servers . . . . . . . . . . . : 10.200.0.2
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Paso 3: Configurar las aplicaciones para que usen la dirección IP privada secundaria

Puede configurar las aplicaciones para que usen la dirección IP privada secundaria. Por ejemplo, si la instancia ejecuta un sitio web en IIS, puede configurar IIS para que use la dirección IP privada secundaria.

Para configurar IIS para el uso de la dirección IP privada secundaria

1. Conéctese a la instancia.
2. Abra el Administrador de Internet Information Services (IIS).
3. En el panel, Conexiones, expanda Sitios.
4. Abra el menú contextual del sitio web (haga clic con el botón derecho) y elija Modificar enlaces.
5. En el cuadro de diálogo Enlaces de sitios, en Tipo, elija http, Modificar.
6. En el cuadro de diálogo Modificar enlace del sitio, en Dirección IP, seleccione la dirección IP privada secundaria. (De manera predeterminada, cada sitio web acepta solicitudes HTTP de todas las direcciones IP).



7. Elija Aceptar, Cerrar.

Nombres de host de instancias de EC2

Al crear una instancia de EC2, AWS crea un nombre de host para esa instancia. Para obtener más información sobre los tipos de nombres de host y cómo los aprovisiona AWS, consulte Tipos de nombres de host de instancias de Amazon EC2. Amazon proporciona un servidor DNS que resuelve los nombres de host proporcionados por Amazon en direcciones IPv4 e IPv6. El servidor DNS de Amazon se encuentra en la base del rango de red de su VPC más dos. Para obtener más información, consulte Atributos de DNS para su VPC en la Guía del usuario de Amazon VPC.

Direcciones de enlace local

Las direcciones de enlace local son direcciones IP conocidas y no enrutables. Amazon EC2 usa direcciones del espacio de direcciones de enlace local para ofrecer servicios a los que solo se puede acceder desde una instancia de EC2. Estos servicios no se ejecutan en la instancia, sino en el host subyacente. Cuando accede a las direcciones de enlace local de estos servicios, se comunica con el hipervisor Xen o con el controlador Nitro.

Rangos de direcciones de enlace local

- IPv4: 169.254.0.0/16 (de 169.254.0.0 a 169.254.255.255)
- IPv6: fe80::/10

Servicios a los que se accede mediante direcciones de enlace local

- Servicio de metadatos de instancias
- Amazon Route 53 Resolver (también conocido como servidor DNS de Amazon)
- Servicio de sincronización temporal de Amazon

Tipos de nombres de host de instancias de Amazon EC2

En esta sección, se describen los tipos de nombre de host del SO invitado de la instancia de Amazon EC2 disponibles al iniciar las instancias en las subredes de la VPC.

El nombre de host distingue las instancias de EC2 de la red. Puede utilizar el nombre de host de una instancia si, por ejemplo, desea ejecutar scripts para comunicarse con algunas o todas las instancias de la red.

Contenido

Tipos de nombres de host de EC2

Hay dos tipos de nombre de host para el nombre de host del SO invitado cuando se inician las instancias de EC2 en una VPC:

- Nombre de IP: el esquema de nomenclatura heredado en el que, al iniciar una instancia, la dirección IPv4 privada de la instancia se incluye en el nombre de host de la instancia. El nombre de IP existe durante toda la vida de la instancia de EC2. Cuando se utiliza como nombre de host DNS privado, solo devolverá la dirección IPv4 privada (registro A).

- Nombre de recurso: al iniciar una instancia, el ID de la instancia de EC2 se incluye en el nombre de host de la instancia. El nombre de recurso existe durante toda la vida de la instancia de EC2. Cuando se usa como nombre de host DNS privado, puede devolver tanto la dirección privada IPv4 (registro A) como la dirección de unidifusión global IPv6 (registro AAAA).

El tipo de nombre de host del SO invitado de la instancia de EC2 depende de la configuración de la subred:

- Si la instancia se inicia en una subred solo IPv4, puede seleccionar el nombre de IP o el nombre de recurso.
- Si la instancia se inicia en una subred de doble pila (IPv4+IPv6), puede seleccionar el nombre de IP o el nombre de recurso.
- Si la instancia se inicia en una subred solo IPv6, se utiliza el nombre de recurso automáticamente.

Contenido

Nombre de IP

Cuando se inicia una instancia de EC2 con el Tipo de nombre de host de Nombre de IP, el nombre de host del SO invitado se configura para utilizar la dirección IPv4 privada.

- Formato de una instancia en us-east-1: *`private-ipv4-address`*`.ec2.internal`
- Ejemplo: *`ip-10-24-34-0`*`.ec2.internal`
- Formato de una instancia en cualquier otra región de AWS: *`private-ipv4-address.region`*`.compute.internal`
- Ejemplo: *`ip-10-24-34-0.us-west-2`*`.compute.internal`

Nombre del recurso

Cuando se inician instancias de EC2 en subredes solo IPv6, el Tipo de nombre de host de Nombre de recurso está seleccionado de forma predeterminada. La opción Nombre de recurso se puede

seleccionar cuando se inicia una instancia en subredes solo IPv4 o de doble pila (IPv4+IPv6). Después de iniciar una instancia, puede administrar la configuración del nombre de host. Para obtener más información, consulte Modificar el tipo de nombre de host y las configuraciones de nombre de host DNS.

Cuando se inicia una instancia de EC2 con el Tipo de nombre de host de Nombre de recurso, el nombre de host del SO invitado se configura para utilizar el ID de la instancia de EC2.

- Formato de una instancia en us-east-1: *ec2-instance-id*.ec2.internal
- Ejemplo: *i-0123456789abcdef*.ec2.internal
- Formato de una instancia en cualquier otra región de AWS: *ec2-instance-id.region*.compute.internal
- Ejemplo: *i-0123456789abcdef.us-west-2*.compute.internal

La diferencia entre el nombre de IP y el nombre de recurso

Las consultas de DNS para nombres de IP y nombres de recurso coexisten para garantizar la compatibilidad con versiones anteriores y permitir la migración de nomenclatura basada en IP para nombres de host a nomenclatura basada en recursos. Para nombres de host DNS privados basados en nombres de IP, no se puede configurar si se responde o no una consulta al registro DNS A para la instancia. Las consultas al registro DNS A siempre se responden independientemente de la configuración del nombre de host del SO invitado. En cambio, para nombres de host DNS privados basados en nombre de recurso, es posible configurar si se responden o no las consultas de DNS A o DNS AAAA para la instancia. El comportamiento de respuesta se configura cuando inicia una instancia o modifica una subred. Para obtener más información, consulte Modificar el tipo de nombre de host y las configuraciones de nombre de host DNS.

Dónde se ve el nombre de recurso y el nombre de IP

En esta sección, se describe dónde puede ver los tipos de nombre de host nombre de recurso y nombre de IP en la consola de EC2.

Contenido

Al crear instancias de EC2

Cuando crea una instancia de EC2, según el tipo de subred que seleccione, el Tipo de nombre de host de Nombre de recurso puede estar disponible o puede que esté seleccionado y no sea modificable. En esta sección, se explican las situaciones en las que puede ver los tipos de nombre de host nombre de recurso y nombre de IP.

Escenario 1

Crea una instancia de EC2 en el asistente (consulte Lance una instancia con el nuevo asistente de inicialización de instancias) y, al configurar los detalles, elige una subred que configuró para que sea solo IPv6.

En este caso, Tipo de nombre de host de Nombre de recurso se selecciona automáticamente y no se puede modificar. La selección de las opciones Nombre de host DNS de Habilitar solicitudes DNS IPv4 de nombre de IP (registro A) e Habilitar solicitudes DNS IPv4 basadas en recursos (registro A) se anulan automáticamente y no se pueden modificar. La opción Habilitar solicitudes DNS IPv6 basadas en recursos (registro AAAA) está seleccionada de forma predeterminada pero es modificable. Si se selecciona, las solicitudes DNS del nombre de recurso se resolverán en la dirección IPv6 (registro AAAA) de esta instancia de EC2.

Escenario 2

Crea una instancia de EC2 en el asistente (consulte Lance una instancia con el nuevo asistente de inicialización de instancias) y, al configurar los detalles, elige una subred configurada con un bloque de CIDR IPv4 o un bloque de CIDR con IPv4 e IPv6 (“pila dual”).

En este caso, Habilitar solicitudes DNS IPv4 de nombre de IP (registro A) se selecciona automáticamente y no se puede cambiar. Esto significa que las solicitudes al nombre IP se resolverán en la dirección IPv4 (registro A) de esta instancia de EC2.

Las opciones están predeterminadas para las configuraciones de la subred, pero puede modificar las opciones de esta instancia en función de la configuración de la subred:

- Tipo de nombre de host: determina si desea que el nombre de host del SO invitado de la instancia de EC2 sea el nombre de recurso o el nombre de IP. El valor predeterminado es Nombre de IP.
- Habilitar solicitudes DNS IPv4 basadas en recursos (registro A): determina si las solicitudes del nombre de recurso se resuelven en la dirección IPv4 privada (registro A) de esta instancia de EC2. Esta opción no está seleccionada de forma predeterminada.

- Enable resource-based IPv6 (AAAA record) DNS requests (Habilitar solicitudes DNS IPv6 basadas en recursos [registro AAAA]): determina si las solicitudes del nombre de recurso se resuelven en la dirección GUA IPv6 (registro AAAA) de esta instancia de EC2. Esta opción no está seleccionada de forma predeterminada.

Al consultar los detalles de una instancia de EC2 existente

Puede ver los valores de nombre de host de una instancia de EC2 existente en la pestaña Detalles de la instancia de EC2:

- Tipo de nombre de host: nombre de host en formato de nombre IP o nombre de recurso.
- Nombre DNS de IP privada (solo IPv4): nombre de IP que siempre se resolverá en la dirección IPv4 privada de la instancia.
- Nombre DNS del recurso privado: nombre de recurso que se resuelve en los registros DNS seleccionados para esta instancia.
- Responder el nombre DNS del recurso privado: el nombre de recurso se resuelve en registros DNS IPv4 (A), IPv6 (AAAA) o IPv4 e IPv6 (A y AAAA).

Además, si se conecta a la instancia de EC2 directamente a través de SSH e ingresa el comando `hostname`, verá el nombre de host en formato de nombre de IP o nombre de recurso.

Cómo decidir si desea elegir el nombre de recurso o el nombre IP

Cuando se inicia una instancia de EC2 (consulte Lance una instancia con el nuevo asistente de inicialización de instancias), si elige un Tipo de nombre de host de Nombre de recurso, la instancia de EC2 se inicia con un nombre de host en formato de nombre de recurso. En tales casos, el registro DNS de esta instancia de EC2 también puede apuntar al nombre de recurso. Esto le da la flexibilidad de elegir si ese nombre de host se resuelve en la dirección IPv4, la dirección IPv6 o la dirección IPv4 e IPv6 de la instancia. Si planea utilizar IPv6 en el futuro o si está utilizando subredes de doble pila hoy, es mejor utilizar un Tipo de nombre de host de Nombre de recurso de modo que cambie la resolución DNS de los nombres de host de las instancias sin realizar ningún cambio en los propios registros DNS. El nombre del recurso le permite agregar y eliminar la resolución DNS IPv4 e IPv6 en una instancia de EC2.

Si, en cambio, elige un Tipo de nombre de host de Nombre de IP, y lo utiliza como el nombre de host DNS, solo se puede resolver en la dirección IPv4 de la instancia. No se resolverá en la dirección IPv6 de la instancia incluso si la instancia tiene una dirección IPv4 y una dirección IPv6 asociadas a ella.

Modificar el tipo de nombre de host y las configuraciones de nombre de host DNS

Siga los pasos de esta sección para modificar las configuraciones de tipo de nombre de host y nombre de host DNS para subredes o instancias de EC2 después de haberse iniciado.

Contenido

Subredes

Modifique las configuraciones de una subred al seleccionar una subred en la consola de VPC y elegir Acciones, Editar la configuración de subred.

> **Note**
>
> Cambiar la configuración de subred no cambia la configuración de las instancias de EC2 que ya se iniciaron en la subred.

- Hostname type (Tipo de nombre de host): determina si desea que la configuración predeterminada del nombre de host del SO invitado de la instancia de EC2 iniciada en la subred sea el nombre de recurso o el nombre IP.
- Habilitar solicitudes de nombre de host DNS IPv4 (registro A): determina si las solicitudes o consultas DNS del nombre del recurso se resuelven en la dirección IPv4 (registro A) de esta instancia de EC2.
- Habilitar solicitudes IPv6 de nombre de host DNS (registro AAAA): determina si las solicitudes o consultas DNS del nombre del recurso se resuelven en la dirección IPv6 (registro AAAA) de esta instancia de EC2.

instancias de EC2

Siga los pasos de esta sección para modificar las configuraciones de tipo de nombre de host y nombre de host DNS de una instancia de EC2.

> **Important**
>
> - Para cambiar la configuración Utilizar la nomenclatura basada en recursos como nombre de host del SO invitado, primero debe detener la instancia. Para cambiar la configuración Responder solicitud de nombre de host DNS IPv4 (registro A) o Responder solicitudes de nombre de host DNS IPv6 (registro AAAA), no es necesario detener la instancia.
> - Para modificar cualquier configuración de los tipos de instancias de EC2 que no están respaldadas por EBS, no puede detener la instancia. Debe terminar la instancia y iniciar una nueva con las configuraciones de nombre de host DNS o tipo de nombre de host deseadas.

Cómo modificar las configuraciones de tipo de nombre de host y nombre de host DNS de una instancia de EC2

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. Si va a cambiar la configuración Utilizar nomenclatura basada en recursos como nombre de host del SO invitado, primero detenga la instancia de EC2. De lo contrario, omita este paso.

   Para detener la instancia, selecciónela y elija Estado de la instancia y Detener instancia.
3. Seleccione la instancia y elija Acciones, Configuración de la instancia, Cambiar las opciones de nomenclatura basada en recursos.

   - Utilizar nomenclatura basada en recursos como nombre de host del SO invitado: determina si desea que el nombre de host del SO invitado de la instancia de EC2 sea el nombre de recurso o el nombre de IP.
   - Responder solicitudes de nombre de host DNS IPv4 (registro A): determina si las solicitudes o consultas DNS del nombre del recurso se resuelven en la dirección IPv4 de esta instancia de EC2.
   - Responder solicitudes de nombre de host DNS IPv6 (registro AAAA): determina si las solicitudes o consultas DNS del nombre del recurso se resuelven en la dirección IPv6 (registro AAAA) de esta instancia de EC2.
4. Seleccione Guardar.
5. Si detuvo la instancia, iníciela de nuevo.

Traiga sus propias direcciones IP (BYOIP) en Amazon EC2

Puede traer todo su rango de direcciones IPv4 o IPv6 direccionables públicamente de su red en las instalaciones a su cuenta de AWS o solo una parte. Usted conserva el control del rango de direcciones y puede anunciarlo en Internet a través de AWS. Una vez que traiga su rango de direcciones a AWS, aparecerá en su cuenta de AWS como un grupo de direcciones.

Para obtener una lista de las regiones en las que la característica Traiga su propia IP (BYOIP) esté disponible, consulte Disponibilidad regional.

> **Note**
>
> - Los pasos en esta página describen cómo traer su propio intervalo de direcciones IP para su uso solo en Amazon EC2.
> - Para traer su propio rango de direcciones IP para su uso en AWS Global Accelerator, consulte Traiga sus propias direcciones IP (BYOIP) en la Guía para desarrolladores de AWS Global Accelerator.
> - Para usar su propio rango de direcciones IP con Amazon VPC IP Address Manager, consulte Tutorial: Cómo convertir sus direcciones IP en IPAM en la Guía del usuario de IPAM de Amazon VPC.

Contenido

Definiciones BYOIP

- Certificado X.509 con autofirma: estándar de certificado utilizado con mayor frecuencia para cifrar y autenticar datos dentro de una red. Es un certificado utilizado por AWS para validar el control sobre el espacio de IP desde un registro RDAP. Para obtener más información sobre los certificados X.509, consulte RFC 3280.
- Número de sistema autónomo (ASN): identificador único mundial que define un grupo de prefijos IP administrados por uno o más operadores de red que mantienen una política de enrutamiento única y claramente definida.
- Registro regional de Internet (RIR): organización que administra la asignación y el registro de direcciones IP y ASN en una región del mundo.
- Protocolo de acceso a datos de registro (RDAP): protocolo de solo lectura para consultar los datos de registro actuales dentro de un RIR. Las entradas de la base de datos de RIR consultada se denominan “registros de RDAP”. Los clientes deben actualizar ciertos tipos de registros mediante un mecanismo proporcionado por el RIR. AWS consulta estos registros para verificar el control de un espacio de direcciones en el RIR.
- Autorización de origen de ruta (ROA): objeto creado por el Registro regional de Internet (RIR) para que los clientes autentiquen la publicidad de IP en sistemas autónomos determinados. Para obtener información general, consulte Route Origin Authorizations (ROAs) en el sitio web de ARIN.
- Registro local de Internet (LIR): organizaciones como proveedores de servicios de Internet que asignan un bloque de direcciones IP de un RIR a sus clientes.

Requisitos y cuotas

- El rango de direcciones debe estar inscrito en el Registro regional de Internet (RIR). Consulte su RIR para conocer las políticas relacionadas con las regiones geográficas. Actualmente, BYOIP permite el Registro Norteamericano de Números de Internet (ARIN), el Centro de Coordinación de Redes IP Europeas (RIPE) o el Centro de Información de Redes de Asia-Pacífico (APNIC). Debe estar registrado con un negocio o entidad institucional y no puede registrarse con el nombre de un individuo.
- El intervalo de direcciones IPv4 más específico que puede traer es /24.
- El intervalo de direcciones IPv6 más específico que puede traer es /48 para los CIDR que se anuncian públicamente y /56 para los CIDR que no se anuncian públicamente.
- Las ROA no son necesarias para los rangos de CIDR que no se anuncian públicamente, pero los registros de RDAP aún deben actualizarse.

- Solo puede traer cada rango de direcciones a una región de AWS de forma simultánea.
- Puede traer un total de cinco rangos de direcciones BYOIP IPv4 e IPv6 por región de AWS a su cuenta de AWS. No puede ajustar las cuotas para los CIDR de BYOIP mediante la consola de Service Quotas, pero puede comunicarse con el Centro de soporte de AWS como se describe en AWS service quotas en Referencia general de AWS.
- No puede compartir su rango de direcciones IP con otras cuentas mediante AWS RAM a menos que utilice el IP Address Manager (IPAM) de Amazon VPC e integre IPAM con AWS Organizations. Para obtener más información, consulte Integración de IPAM con AWS Organizations en la Guía del usuario de Amazon VPC IPAM.
- Las direcciones del rango de direcciones IP deben tener un historial limpio. Podemos investigar la reputación del intervalo de direcciones IP y reservarnos el derecho a rechazar un intervalo de direcciones IP si contiene una dirección IP con una mala reputación o asociada a un comportamiento malicioso.
- El espacio de direcciones heredado, el espacio de direcciones IPv4 distribuido por el registro central de la Autoridad de Números Asignados de Internet (IANA) antes de la creación del sistema de Registro regional de Internet (RIR), aún requiere el objeto ROA correspondiente.
- En el caso de los LIR, es común que utilicen un proceso manual para actualizar sus registros. Esto puede tardar días en implementarse en función del LIR.
- Se necesita un único objeto ROA y un registro de RDAP para un bloque de CIDR grande. Puede traer varios bloques de CIDR más pequeños de ese rango a AWS, incluso en varias regiones de AWS, con el objeto único y el registro.
- El BYOIP no es compatible en zonas de Wavelength o en AWS Outposts.
- No realice ningún cambio manual para BYOIP en la base de datos de activos de enrutamiento (RADb) ni en ningún otro IRR. BYOIP actualizará automáticamente la RADb. Cualquier cambio manual que incluya el ASN de BYOIP provocará un error en la operación de aprovisionamiento de BYOIP.
- Una vez que haya llevado un rango de direcciones IPv4 aAWS, podrá usar todas las direcciones IP del rango, incluidas la primera dirección (la dirección de red) y la última dirección (la dirección de transmisión).

Requisitos previos de incorporación para su rango de direcciones BYOIP

El proceso de incorporación de BYOIP tiene dos fases, para las cuales debe realizar tres pasos. Estos pasos corresponden a los pasos descritos en el siguiente diagrama. Incluimos pasos manuales

en esta documentación, pero su RIR puede ofrecer servicios administrados para ayudarlo con estos pasos.

Fase de preparación

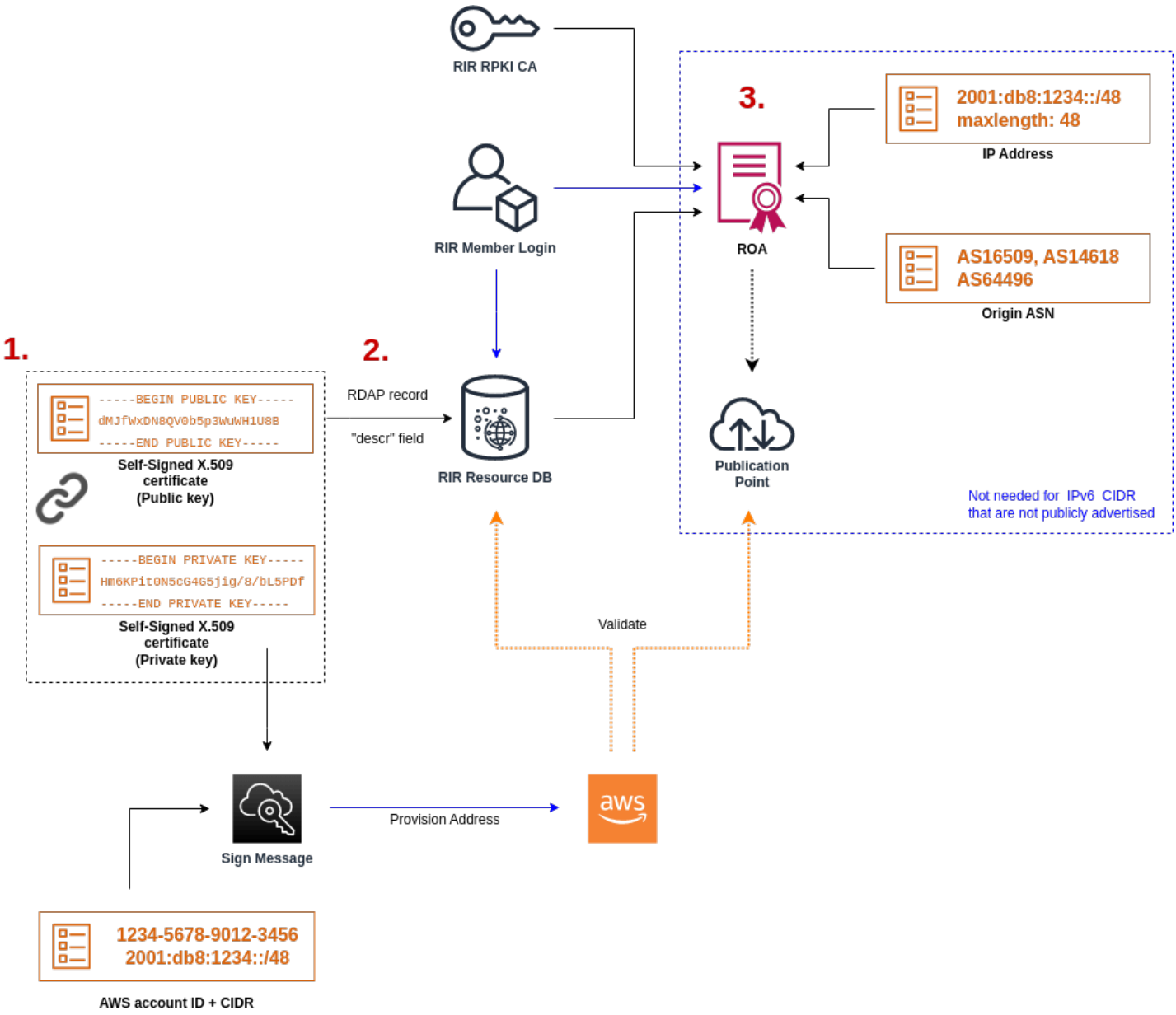
1. Cree una clave privada y úsela para generar un certificado X.509 autofirmado para fines de autenticación. Este certificado solo se usa durante la fase de aprovisionamiento.

Fase de configuración del RIR

2. Cargue el certificado autofirmado en los comentarios del registro de RDAP.

3. Cree un objeto ROA en su Registro Regional de Internet (RIR). La autorización de origen de ruta (ROA) define el rango de direcciones deseado, los números de sistema autónomo (ASN) permitidos para anunciar el rango de direcciones y una fecha de vencimiento para registrarse en la infraestructura de clave pública de recursos (RPKI) de su RIR.

> **Note**
>
> No se requiere una ROA para el espacio de direcciones IPv6 que no se anuncia públicamente.



Para incorporar varios rangos de direcciones no contiguos, debe repetir este proceso con cada rango de direcciones. Sin embargo, no es necesario repetir los pasos de preparación y de configuración del RIR si se divide un bloque contiguo en varias regiones de AWS diferentes.

La incorporación de un rango de direcciones no tiene ningún efecto en ninguno de los rangos de direcciones que haya incorporado con anterioridad.

> **Important**
>
> Antes de incorporar el rango de direcciones, complete los siguientes requisitos previos. Las tareas de esta sección requieren un terminal Linux y se pueden realizar mediante Linux, AWS CloudShell o el Subsistema de Windows para Linux.

1. Cree una clave privada y genere un certificado X.509

Use el siguiente procedimiento para crear un certificado autofirmado X.509 y agréguelo al registro de RDAP para su RIR. Este par de claves se utiliza para autenticar el rango de direcciones con el RIR. Los comandos openssl requieren la versión 1.0.2 o posterior de OpenSSL.

Copie los comandos siguientes y reemplace solo los valores del marcador de posición (en cursiva y de color).

Este procedimiento sigue la práctica recomendada de cifrar su clave de RSA privada y de requerir una frase de contraseña para acceder a ella.

1. Genere una clave RSA privada de 2048 bits del siguiente modo.

```
$ openssl genpkey -aes256 -algorithm RSA -pkeyopt rsa_keygen_bits:2048 -out
 private-key.pem
```

   El parámetro `-aes256` especifica el algoritmo utilizado para cifrar la clave privada. El comando devuelve el siguiente resultado, incluidos los pedidos para establecer una frase de contraseña:

```
......+++
.+++
Enter PEM pass phrase: xxxxxxx
Verifying - Enter PEM pass phrase: xxxxxxx
```

   Puede inspeccionar la clave mediante el siguiente comando:

```
$ openssl pkey -in private-key.pem -text
```

   Esto devuelve un pedido de frase de contraseña y el contenido de la clave, que debería ser similar a lo siguiente:

```
Enter pass phrase for private-key.pem: xxxxxxx
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDFBXHRI4HVKAhh
3seiciooizCRTbJe1+YsxNTja4XyKypVGIFWDGhZs44FCHlPOOSVJ+NqP74w96oM
7DPS3xo9kaQyZBFn2YEp2EBq5vf307KHNRmZZUmkn0zHOSEpNmY2fMxISBxewlxR
FAniwmSd/8TDvHJMY9FvAIvWuTsv5l0tJKk+a91K4+tO3UdDR7Sno5WXExfsBrW3
g1ydo3TBsx8i5/YiVOcNApy7ge2/FiwY3aCXJB6r6nuF6H8mRgI4r4vkMRsOlAhJ
DnZPNeweboo+K3Q3lwbgbmOKD/z9svk8N/+hUTBtIX0fRtbG+PLIw3xWRHGrMSn2
BzsPVuDLAgMBAAECggEACiJUj2hfJkKv47Dc3es3Zex67A5uDVjXmxfox2Xhdupn
fAcNqAptV6fXt0SPUNbhUxbBKNbshoJGufFwXPli1SXnpzvkdU4Hyco4zgbhXFsE
RNYjYfOGzTPwdBLpNMB6k3Tp4RHse6dNrlH0jDhpioL8cQEBdBJyVF5X0wymEbmV
mC0jgH/MxsBAPWW6ZKicg9ULMlWiAZ3MRAZPjHHgpYkAAsUWKAbCBwVQcVjGO59W
jfZjzTX5pQtVVH68ruciH88DTZCwjCkjBhxg+OIkJBLE5wkh82jIHSivZ63flwLw
z+E0+HhELSZJrn2MY6Jxmik3qNNUOF/Z+3msdj2luQKBgQDjwlC/3jxp8zJy6P8o
JQKv7TdvMwUj4VSWOHZBHLv4evJaaia0uQjIo1UDa8AYitqhX1NmCCehGH8yuXj/
v6V3CzMKDkmRr1NrONnSz5QsndQ04Z6ihAQlPmJ96g4wKtgoC7AYpyP0g1a+4/sj
b1+o3YQI4pD/F71c+qaztH7PRwKBgQDdc23yNmT3+Jyptf0fKjEvONK+xwUKzi9c
L/OzBq5yOIC1Pz2T85gOe1i8kwZws+xlpG6uBT6lmIJELd0k59FyupNu4dPvX5SD
6GGqdx4jk9KvI74usGeOBohmF0phTHkrWKBxXiyT0oS8zjnJlEn8ysIpGgO28jjr
LpaHNZ/MXQKBgQDfLNcnS0LzpsS2aK0tzyZU8SMyqVHOGMxj7quhneBq2T6FbiLD
T9TVlYaGNZ0j71vQaLI19qOubWymbautH0Op5KV8owdf4+bf1/NJaPIOzhDUSIjD
Qo01WW31Z9XDSRhKFTnWzmCjBdeIcajyzf10YKsycaAW9lItu8aBrMndnQKBgQDb
nNp/JyRwqjOrNljk7DHEs+SD39kHQzzCfqd+dnTPv2sc06+cpym3yulQcbokULpy
fmRo3bin/pvJQ3aZX/Bdh9woTXqhXDdrrSwWInVYMQPyPk8f/D9mIOJp5FUWMwHD
U+whIZSxsEeE+jtixlWtheKRYkQmzQZXbWdIhYyI3QKBgD+F/6wcZ85QW8nAUykA
3WrSIx/3cwDGdm4NRGct8ZOZjTHjiy9ojMOD1L7iMhRQ/3k3hUsin5LDMp/ryWGG
x4uIaLat40kiC7T4I66DM7P59euqdz3w0PD+VU+h7GSivvsFDdySUt7bNK0AUVLh
dMJfWxDN8QV0b5p3WuWH1U8B
-----END PRIVATE KEY-----
Private-Key: (2048 bit)
modulus:
    00:c5:05:71:d1:23:81:d5:28:08:61:de:c7:a2:72:
    2a:28:8b:30:91:4d:b2:5e:d7:e6:2c:c4:d4:e3:6b:
    85:f2:2b:2a:55:18:81:56:0c:68:59:b3:8e:05:08:
    79:4f:38:e4:95:27:e3:6a:3f:be:30:f7:aa:0c:ec:
    33:d2:df:1a:3d:91:a4:32:64:11:67:d9:81:29:d8:
    40:6a:e6:f7:f7:d3:b2:87:35:19:99:65:49:a4:9f:
    4c:c7:39:21:29:36:66:36:7c:cc:48:48:1c:5e:c2:
    5c:51:14:09:e2:c2:64:9d:ff:c4:c3:bc:72:4c:63:
    d1:6f:00:8b:d6:b9:3b:2f:e6:5d:2d:24:a9:3e:6b:
    dd:4a:e3:eb:4e:dd:47:43:47:b4:a7:a3:95:97:13:
    17:ec:06:b5:b7:83:5c:9d:a3:74:c1:b3:1f:22:e7:
    f6:22:54:e7:0d:02:9c:bb:81:ed:bf:16:2c:18:dd:
```

```
    a0:97:24:1e:ab:ea:7b:85:e8:7f:26:46:02:38:af:
    8b:e4:31:1b:0e:94:08:49:0e:76:4f:35:ec:1e:6e:
    8a:3e:2b:74:37:97:06:e0:6e:63:8a:0f:fc:fd:b2:
    f9:3c:37:ff:a1:51:30:6d:21:7d:1f:46:d6:c6:f8:
    f2:c8:c3:7c:56:44:71:ab:31:29:f6:07:3b:0f:56:
    e0:cb
publicExponent: 65537 (0x10001)
privateExponent:
    0a:22:54:8f:68:5f:26:42:af:e3:b0:dc:dd:eb:37:
    65:ec:7a:ec:0e:6e:0d:58:d7:9b:17:e8:c7:65:e1:
    76:ea:67:7c:07:0d:a8:0a:6d:57:a7:d7:b7:44:8f:
    50:d6:e1:53:16:c1:28:d6:ec:86:82:46:b9:f1:70:
    5c:f9:62:d5:25:e7:a7:3b:e4:75:4e:07:c9:ca:38:
    ce:06:e1:5c:5b:04:44:d6:23:61:f3:86:cd:33:f0:
    74:12:e9:34:c0:7a:93:74:e9:e1:11:ec:7b:a7:4d:
    ae:51:f4:8c:38:69:8a:82:fc:71:01:01:74:12:72:
    54:5e:57:d3:0c:a6:11:b9:95:98:2d:23:80:7f:cc:
    c6:c0:40:3d:65:ba:64:a8:9c:83:d5:0b:32:55:a2:
    01:9d:cc:44:06:4f:8c:71:e0:a5:89:00:02:c5:16:
    28:06:c2:07:05:50:71:58:c6:3b:9f:56:8d:f6:63:
    cd:35:f9:a5:0b:55:54:7e:bc:ae:e7:22:1f:cf:03:
    4d:90:b0:8c:29:23:06:1c:60:f8:e2:24:24:12:c4:
    e7:09:21:f3:68:c8:1d:28:af:67:ad:df:97:02:f0:
    cf:e1:34:f8:78:44:2d:26:49:ae:7d:8c:63:a2:71:
    9a:29:37:a8:d3:54:38:5f:d9:fb:79:ac:76:3d:a5:
    b9
prime1:
    00:e3:c2:50:bf:de:3c:69:f3:32:72:e8:ff:28:25:
    02:af:ed:37:6f:33:05:23:e1:54:96:38:76:41:1c:
    bb:f8:7a:f2:5a:6a:26:b4:b9:08:c8:a3:55:03:6b:
    c0:18:8a:da:a1:5f:53:66:08:27:a1:18:7f:32:b9:
    78:ff:bf:a5:77:0b:33:0a:0e:49:91:af:53:6b:38:
    d9:d2:cf:94:2c:9d:d4:34:e1:9e:a2:84:04:25:3e:
    62:7d:ea:0e:30:2a:d8:28:0b:b0:18:a7:23:f4:83:
    56:be:e3:fb:23:6f:5f:a8:dd:84:08:e2:90:ff:17:
    bd:5c:fa:a6:b3:b4:7e:cf:47
prime2:
    00:dd:73:6d:f2:36:64:f7:f8:9c:a9:b5:fd:1f:2a:
    31:2f:38:d2:be:c7:05:0a:ce:2f:5c:2f:f3:b3:06:
    ae:72:38:80:b5:3f:3d:93:f3:98:0e:7b:58:bc:93:
    06:70:b3:ec:65:a4:6e:ae:05:3e:a5:98:82:44:2d:
    dd:24:e7:d1:72:ba:93:6e:e1:d3:ef:5f:94:83:e8:
    61:aa:77:1e:23:93:d2:af:23:be:2e:b0:67:8e:06:
    88:66:17:4a:61:4c:79:2b:58:a0:71:5e:2c:93:d2:
```

```
    84:bc:ce:39:c9:94:49:fc:ca:c2:29:1a:03:b6:f2:
    38:eb:2e:96:87:35:9f:cc:5d
exponent1:
    00:df:2c:d7:27:4b:42:f3:a6:c4:b6:68:ad:2d:cf:
    26:54:f1:23:32:a9:51:ce:18:cc:63:ee:ab:a1:9d:
    e0:6a:d9:3e:85:6e:22:c3:4f:d4:d5:95:86:86:35:
    9d:23:ef:5b:d0:68:b2:35:f6:a3:ae:6d:6c:a6:6d:
    ab:ad:1f:43:a9:e4:a5:7c:a3:07:5f:e3:e6:df:d7:
    f3:49:68:f2:0e:ce:10:d4:48:88:c3:42:8d:35:59:
    6d:f5:67:d5:c3:49:18:4a:15:39:d6:ce:60:a3:05:
    d7:88:71:a8:f2:cd:fd:74:60:ab:32:71:a0:16:f6:
    52:2d:bb:c6:81:ac:c9:dd:9d
exponent2:
    00:db:9c:da:7f:27:24:70:aa:33:ab:36:58:e4:ec:
    31:c4:b3:e4:83:df:d9:07:43:3c:c2:7e:a7:7e:76:
    74:cf:bf:6b:1c:d3:af:9c:a7:29:b7:ca:e9:50:71:
    ba:24:50:ba:72:7e:64:68:dd:b8:a7:fe:9b:c9:43:
    76:99:5f:f0:5d:87:dc:28:4d:7a:a1:5c:37:6b:ad:
    2c:16:22:75:58:31:03:f2:3e:4f:1f:fc:3f:66:20:
    e2:69:e4:55:16:33:01:c3:53:ec:21:21:94:b1:b0:
    47:84:fa:3b:62:c6:55:ad:85:e2:91:62:44:26:cd:
    06:57:6d:67:48:85:8c:88:dd
coefficient:
    3f:85:ff:ac:1c:67:ce:50:5b:c9:c0:53:29:00:dd:
    6a:d2:23:1f:f7:73:00:c6:76:6e:0d:44:67:2d:f1:
    93:99:8d:31:e3:8b:2f:68:8c:c3:83:d4:be:e2:32:
    14:50:ff:79:37:85:4b:22:9f:92:c3:32:9f:eb:c9:
    61:86:c7:8b:88:68:b6:ad:e3:49:22:0b:b4:f8:23:
    ae:83:33:b3:f9:f5:eb:aa:77:3d:f0:d0:f0:fe:55:
    4f:a1:ec:64:a2:be:fb:05:0d:dc:92:52:de:db:34:
    ad:00:51:52:e1:74:c2:5f:5b:10:cd:f1:05:74:6f:
    9a:77:5a:e5:87:d5:4f:01
```

Mantenga su clave privada en un lugar seguro cuando no la esté utilizando.

2. Genere un certificado X.509 con la clave privada que creó en el paso anterior. En este ejemplo, el certificado vence en 365 días. Pasada dicha cantidad de días, no será fiable. Asegúrese de fijar la fecha de vencimiento en concordancia. El certificado solo debe ser válido durante el proceso de aprovisionamiento. Puede eliminar el certificado del registro de su RIR una vez que se haya completado la etapa de aprovisionamiento. El comando `tr -d "\n"` elimina caracteres de nueva línea (saltos de línea) del resultado. Cuando se le solicite, debe proporcionar un nombre común, pero los demás campos se pueden dejar en blanco.

```
$ openssl req -new -x509 -key private-key.pem -days 365 | tr -d "\n" >
 certificate.pem
```

Esto devuelve un resultado similar a lo siguiente:

```
Enter pass phrase for private-key.pem: xxxxxxx
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:
State or Province Name (full name) []:
Locality Name (eg, city) []:
Organization Name (eg, company) []:
Organizational Unit Name (eg, section) []:
Common Name (eg, fully qualified host name) []:example.com
Email Address []:
```

> **Note**
>
> El nombre común no es necesario para el aprovisionamiento de AWS. Puede ser cualquier nombre de dominio interno o público.

Puede inspeccionar el certificado con el siguiente comando:

```
$ cat certificate.pem
```

El resultado debe ser una cadena larga, codificada en PEM, sin saltos de línea, precedida por `-----BEGIN CERTIFICATE-----` y seguida por `-----END CERTIFICATE-----`.

2. Cargue el certificado X.509 al registro RDAP de su RIR

Agregue el certificado que creó anteriormente al registro de RDAP para su RIR. Asegúrese de incluir las cadenas `-----BEGIN CERTIFICATE-----` y `-----END CERTIFICATE-----` antes

y después de la parte codificada. Todo este contenido debe estar en una sola línea larga. El procedimiento para actualizar el RDAP depende de su RIR:

- Para ARIN, utilice el portal del administrador de cuentas para agregar el certificado en la sección "Comentarios públicos" del objeto "Información de red" que representa su rango de direcciones. No lo añada a la sección de comentarios de su organización.
- Para RIPE, agregue el certificado como un nuevo campo "descr" al objeto "inetnum" o "inet6num" que representa su rango de direcciones. Por lo general, se encuentran en la sección "Mis recursos" del portal de bases de datos de RIPE. No lo agregue a la sección de comentarios de la organización ni al campo "comentarios" de los objetos anteriores.
- Para APNIC, envíe el certificado por correo electrónico a helpdesk@apnic.net para agregarla manualmente al campo "observaciones". Envíe el correo electrónico con el contacto autorizado de APNIC para las direcciones IP.

Puede eliminar el certificado del registro de su RIR una vez que se haya completado la siguiente etapa de aprovisionamiento.

3. Creación de un objeto ROA en su Registro Regional de Internet (RIR)

Cree un objeto ROA para permitir que los ASN de Amazon 16509 y 14618 anuncien su rango de direcciones, así como también los ASN que cuentan actualmente con autorización para anunciar el rango de direcciones. Para AWS GovCloud (US) Regions, autorice ASN 8987 en lugar de 16509 y 14618. Se debe fijar la longitud máxima en función del tamaño del CIDR que traiga. El prefijo IPv4 más específico que puede traer es /24. El intervalo de direcciones IPv6 más específico que puede traer es /48 para los CIDR que se anuncian públicamente y /56 para los CIDR que no se anuncian públicamente.

> **Important**
>
> Si va a crear un objeto ROA para Amazon VPC IP Address Manager (IPAM), al crear los ROA, para los CIDR de IPv4 debe establecer la longitud máxima de un prefijo de dirección IP en `/24`. Para los CIDR IPv6, si los agregará a un grupo que se puede anunciar, la longitud máxima de un prefijo de dirección IP debe ser `/48`. Esto garantiza que tenga total flexibilidad para dividir su dirección IP pública entre regiones de AWS. IPAM impone la longitud máxima que establezca. Para obtener más información sobre las direcciones BYOIP para IPAM, consulte Tutorial: CIDR con dirección BYOIP a IPAM en la Guía del usuario de Amazon VPC IPAM.

Es posible que pasen 24 horas hasta que la ROA esté disponible en Amazon. Para obtener más información, consulte su RIR:

- ARIN — ROA Requests
- RIPE — Managing ROAs
- APNIC — Route Management

Al migrar anuncios desde una carga de trabajo en las instalaciones a AWS, debe crear una ROA para su ASN existente antes de crear las ROA para los ASN de Amazon. De lo contrario, podría afectar al enrutamiento y a los anuncios existentes.

> **Important**
>
> Para que Amazon anuncie y siga anunciando su intervalo de direcciones IP, sus ROA con los ASN de Amazon deben cumplir con las directrices anteriores. Si sus ROA no son válidas o no cumplen con las normas anteriores, Amazon se reserva el derecho de dejar de anunciar su rango de direcciones IP.

> **Note**
>
> Este paso no se requiere para el espacio de direcciones IPv6 que no se anuncia públicamente.

Incorporación de su BYOIP

El proceso de incorporación de BYOIP incluye las siguientes tareas en función de sus necesidades.

Tareas

- Aprovisione un intervalo de direcciones que se anuncie públicamente en AWS
- Aprovisione un intervalo de direcciones IPv6 que no se anuncie públicamente
- Anunciar el rango de direcciones mediante AWS
- Desaprovisionar el rango de direcciones

Aprovisione un intervalo de direcciones que se anuncie públicamente en AWS

Cuando aprovisiona un rango de direcciones para utilizarlo con AWS, usted confirma que controla el rango de direcciones y autoriza que Amazon lo anuncie. También verificamos que controla el rango de direcciones a través de un mensaje de autorización firmado. Este mensaje se firma con el par de claves autofirmado X.509 que utilizó cuando actualizó el registro de RDAP con el certificado X.509. AWS requiere un mensaje de autorización firmado criptográficamente que presenta al RIR. El RIR autentica la firma con el certificado que agregó al RDAP y verifica los detalles de autorización con la ROA.

Para aprovisionar el rango de direcciones

1. Redactar mensajes

   Redacte el mensaje de autorización de texto sin formato. El formato del mensaje es el siguiente, donde la fecha es la fecha de vencimiento del mensaje:

   ```
   1|aws|account|cidr|YYYYMMDD|SHA256|RSAPSS
   ```

   Reemplace el número de cuenta, el rango de direcciones y la fecha de vencimiento con sus propios valores para crear un mensaje similar al siguiente:

   ```
   text_message="1|aws|0123456789AB|198.51.100.0/24|20211231|SHA256|RSAPSS"
   ```

   Esto no debe confundirse con un mensaje de ROA, que es similar.

2. Firmar el mensaje

   Firme el mensaje de texto sin formato con la clave privada que creó anteriormente. La firma que devuelve este comando es una cadena larga que deberá usar en el siguiente paso.

   > **Important**
   >
   > Le recomendamos que copie y pegue este comando. Excepto por el contenido del mensaje, no modifique ni reemplace ninguno de los valores.

```
signed_message=$( echo -n $text_message | openssl dgst -sha256 -sigopt
 rsa_padding_mode:pss -sigopt rsa_pss_saltlen:-1 -sign private-key.pem -keyform PEM
 | openssl base64 | tr -- '+=/' '-_~' | tr -d "\n")
```

3. Aprovisionar la dirección

   Para aprovisionar el rango de direcciones, use el comando provision-byoip-cidr de la AWS CLI. La opción `--cidr-authorization-context` utiliza las cadenas de mensaje y firma que creó anteriormente.

   > **Important**
   >
   > Debe especificar la región de AWS en la que se debe aprovisionar el rango de BYOIP si difiere de la configuración de la AWS CLI `Default region name`.

   ```
   aws ec2 provision-byoip-cidr --cidr address-range --cidr-authorization-context
    Message="$text_message",Signature="$signed_message" --region us-east-1
   ```

   Aprovisionar un rango de direcciones es una operación asincrónica, por lo que la llamada se devuelve de forma inmediata, pero el rango de direcciones no se podrá utilizar hasta que su estado pase de `pending-provision` a `provisioned`.

4. Monitorear el progreso

   Si bien la mayoría del aprovisionamiento se completará en dos horas, el proceso de aprovisionamiento de los intervalos que se pueden anunciar públicamente puede tardar hasta una semana en completarse. Utilice el comando describe-byoip-cidrs para monitorear el progreso, como en este ejemplo:

   ```
   aws ec2 describe-byoip-cidrs --max-results 5 --region us-east-1
   ```

   Si hay problemas durante el aprovisionamiento y el estado pasa a `failed-provision`, debe ejecutar el comando `provision-byoip-cidr` de nuevo una vez que se hayan resuelto los problemas.

Aprovisione un intervalo de direcciones IPv6 que no se anuncie públicamente

De forma predeterminada, se aprovisiona un intervalo de direcciones para que se anuncie públicamente en Internet. Puede aprovisionar un intervalo de direcciones IPv6 que no se anunciará públicamente. Para las rutas que no son anunciables públicamente, el proceso de aprovisionamiento generalmente se completa en cuestión de minutos. Cuando asocia un bloque de CIDR IPv6 de un rango de direcciones no público a una VPC, solo se puede acceder al CIDR IPv6 a través de opciones de conectividad híbrida que admiten IPv6, como AWS Direct Connect, AWS Site-to-Site VPN o puertas de enlace de tránsito de Amazon VPC.

No se requiere una ROA para aprovisionar un intervalo de direcciones no públicas.

> **Important**
>
> - Solo puede especificar si un intervalo de direcciones se anuncia públicamente durante el aprovisionamiento. No puede cambiar el estado anunciable de un rango de direcciones con posterioridad.
> - Amazon VPC no admite los CIDR de direcciones locales únicas (ULA). Todas las VPC deben tener CIDR de IPv6 únicos. Dos VPC no pueden tener el mismo rango de CIDR de IPv6.

Para aprovisionar un intervalo de direcciones IPv6 que no se anunciará públicamente, use el siguiente comando provision-byoip-cidr.

```
aws ec2 provision-byoip-cidr --cidr address-range --cidr-authorization-context
 Message="$text_message",Signature="$signed_message" --no-publicly-advertisable --
region us-east-1
```

Anunciar el rango de direcciones mediante AWS

Una vez aprovisionado el rango de direcciones, ya se puede anunciar. Debe anunciar el rango de direcciones exacto que ha aprovisionado. No puede anunciar solo una parte del rango de direcciones aprovisionado.

Si ha aprovisionado un intervalo de direcciones IPv6 que no se anunciará públicamente, no es necesario que complete este paso.

Le recomendamos que deje de anunciar el rango de direcciones o una parte de él desde otras ubicaciones antes de anunciarlo a través de AWS. Si sigue anunciando su rango de direcciones IP o una parte de él desde otras ubicaciones, no podremos asistirle de forma fiable ni solucionar los problemas. En especial, no podremos garantizar que el tráfico hacia el rango de direcciones o una parte de él entre en nuestra red.

Para minimizar el tiempo de inactividad, puede configurar sus recursos de AWS para que utilicen una dirección de su grupo de direcciones antes de que se anuncie. Luego puede dejar de anunciarla de forma simultánea desde la ubicación actual y empezar a anunciarla a través de AWS. Para obtener más información acerca de cómo asignar una dirección IP elástica desde su grupo de direcciones, consulte Asignar una dirección IP elástica.

Limitaciones

- Puede ejecutar el comando advertise-byoip-cidr como mucho una vez cada 10 segundos, incluso si indica rangos de direcciones diferentes cada vez.
- Puede ejecutar el comando withdraw-byoip-cidr como mucho una vez cada 10 segundos, incluso si indica rangos de direcciones diferentes cada vez.

Para anunciar el rango de direcciones, use el siguiente comando advertise-byoip-cidr.

```
aws ec2 advertise-byoip-cidr --cidr address-range --region us-east-1
```

Para dejar de anunciar el rango de direcciones, use el siguiente comando withdraw-byoip-cidr.

```
aws ec2 withdraw-byoip-cidr --cidr address-range --region us-east-1
```

Desaprovisionar el rango de direcciones

Para dejar de utilizar el rango de direcciones con AWS, primero libere las direcciones IP elásticas y desasocie los bloques de CIDR IPv6 que todavía estén asignados del grupo de direcciones. A continuación, deje de anunciar el intervalo de direcciones y, finalmente, desaprovisione el intervalo de direcciones.

No puede desaprovisionar una parte del intervalo de direcciones. Si desea utilizar un rango de direcciones más específico con AWS, desaprovisione todo el rango de direcciones y aprovisione un rango de direcciones más específico.

(IPv4) Para liberar cada dirección IP elástica, utilice el siguiente comando release-address.

```
aws ec2 release-address --allocation-id eipalloc-12345678abcabcabc --region us-east-1
```

(IPv6) Para desasociar un bloque de CIDR IPv6, utilice el siguiente comando disassociate-vpc-cidr-block.

```
aws ec2 disassociate-vpc-cidr-block --association-id vpc-cidr-assoc-12345abcd1234abc1
 --region us-east-1
```

Para dejar de anunciar el rango de direcciones, use el siguiente comando withdraw-byoip-cidr.

```
aws ec2 withdraw-byoip-cidr --cidr address-range --region us-east-1
```

Para desaprovisionar el rango de direcciones, use el siguiente comando deprovision-byoip-cidr.

```
aws ec2 deprovision-byoip-cidr --cidr address-range --region us-east-1
```

Puede tardar hasta un día en desaprovisionar un intervalo de direcciones.

Uso del intervalo de direcciones

Puede ver y usar los rangos de direcciones IPv4 e IPv6 que haya aprovisionado en su cuenta.

Intervalos de direcciones IPv4

Puede crear una dirección IP elástica a partir de su grupo de direcciones IPv4 y utilizarla con los recursos de AWS como las instancias de EC2, las puertas de enlace de NAT y los Equilibradores de carga de red.

Para ver información sobre los grupos de direcciones IPv4 que ha aprovisionado en su cuenta, utilice el siguiente comando describe-public-ipv4-pools.

```
aws ec2 describe-public-ipv4-pools --region us-east-1
```

Para crear una dirección IP elástica en su grupo de direcciones IPv4, use el comando allocate-address. Puede usar la opción `--public-ipv4-pool` para especificar el ID del grupo de direcciones devuelto por `describe-byoip-cidrs`. O puede usar la opción `--address` para especificar una dirección del rango de direcciones que ha aprovisionado.

Intervalos de direcciones IPv6

Para ver información sobre los grupos de direcciones IPv6 que ha aprovisionado en su cuenta, utilice el siguiente comando describe-ipv6-pools.

```
aws ec2 describe-ipv6-pools --region us-east-1
```

Para crear una VPC y especificar un CIDR IPv6 desde el grupo de direcciones IPv6, utilice el siguiente comando create-vpc. Para permitir que Amazon elija el CIDR IPv6 de su grupo de direcciones IPv6, omita la opción `--ipv6-cidr-block`.

```
aws ec2 create-vpc --cidr-block 10.0.0.0/16 --ipv6-cidr-block ipv6-cidr --ipv6-
pool pool-id --region us-east-1
```

Para asociar un bloque de CIDR IPv6 del grupo de direcciones IPv6 a una VPC, utilice el siguiente comando associate-vpc-cidr-block. Para permitir que Amazon elija el CIDR IPv6 de su grupo de direcciones IPv6, omita la opción `--ipv6-cidr-block`.

```
aws ec2 associate-vpc-cidr-block --vpc-id vpc-123456789abc123ab --ipv6-cidr-block ipv6-
cidr --ipv6-pool pool-id --region us-east-1
```

Para ver las VPC y la información del grupo de direcciones IPv6 asociada, utilice el comando describe-vpcs. Para ver información acerca de los bloques de CIDR IPv6 asociados de un grupo de direcciones IPv6 específico, utilice el siguiente comando get-associated-ipv6-pool-cidrs.

```
aws ec2 get-associated-ipv6-pool-cidrs --pool-id pool-id --region us-east-1
```

Si desasocia el bloque de CIDR IPv6 de la VPC, se vuelve a liberar en el grupo de direcciones IPv6.

Validación de su BYOIP

1. Validación del par de claves del X.509 autofirmado

   Valide que el certificado se ha cargado y es válido a través del comando whois.

   Para ARIN, utilice `whois -h whois.arin.net r + 2001:0DB8:6172::/48` para buscar el registro de RDAP para su rango de direcciones. Compruebe la sección `Public Comments` para el `NetRange` (rango de red) en la salida del comando. El certificado debe agregarse en la sección `Public Comments` para el rango de direcciones.

Puede inspeccionar la sección `Public Comments` que contiene el certificado con el siguiente comando:

```
whois -h whois.arin.net r + 2001:0DB8:6172::/48 | grep Comments | grep BEGIN
```

Esto devuelve un resultado con el contenido de la clave, que debería ser similar a lo siguiente:

```
Public Comments:
-----BEGIN CERTIFICATE-----
MIID1zCCAr+gAwIBAgIUBkRPNSLrPqbRAFP8RDAHSP+I1TowDQYJKoZIhvcNAQE
LBQAwezELMAkGA1UEBhMCTloxETAPBgNVBAgMCEF1Y2tsYW5kMREwDwYDVQQHDA
hBdWNrbGFuZDEcMBoGA1UECgwTQW1hem9uIFdlYiBTZXJ2aWNlczETMBEGA1UEC
wwKQllPSVAgRGVtbzETMBEGA1UEAwwKQllPSVAgRGVtbzAeFw0yMTEyMDcyMDI0
NTRaFw0yMjEyMDcyMDI0NTRaMHsxCzAJBgNVBAYTAk5aMREwDwYDVQQIDAhBdWN
rbGFuZDERMA8GA1UEBwwIQXVja2xhbmQxHDAaBgNVBAoME0FtYXpvbiBXZWIgU2
VydmljZXMxEzARBgNVBAsMCkJZT0lQIERlbW8xEzARBgNVBAMMCkJZT0lQIERlb
W8wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCfmacvDp0wZ0ceiXXc
R/q27mHI/U5HKt7SST4X2eAqufR9wXkfNanAEskgAseyFypwEEQr4CJijI/5hp9
prh+jsWHWwkFRoBRR9FBtwcU/45XDXLga7D3stsI5QesHVRwOaXUdprAnndaTug
mDPkD0vrl475JWDSIm+PUxGWLy+60aBqiaZq35wU/x+wXlAqBXg4MZK2KoUu27k
Yt2zhmy0S7Ky+oRfRJ9QbAiSu/RwhQbh5Mkp1ZnVIc7NqnhdeIW48QaYjhMlUEf
xdaqYUinzz8KpjfADZ4Hvqj9jWZ/eXo/9b2rGlHWkJsbhr0VEUyAGu1bwkgcdww
3A7NjOxQbAgMBAAGjUzBRMB0GA1UdDgQWBBStFyujN6SYBr2glHpGt0XGF7GbGT
AfBgNVHSMEGDAWgBStFyujN6SYBr2glHpGt0XGF7GbGTAPBgNVHRMBAf8EBTADA
QH/MA0GCSqGSIb3DQEBCwUAA4IBAQBX6nn6YLhz521lfyVfxY0t6o3410bQAeAF
08ud+ICtmQ4IO4A4B7zV3zIVYr0clrOOaFyLxngwMYN0XY5tVhDQqk4/gmDNEKS
Zy2QkX4Eg0YUWVzOyt6fPzjOvJLcsqc1hcF9wySL507XQz76Uk5cFypBOzbnk35
UkWrzA9KK97cXckfIESgK/k1N4ecwxwG6VQ8mBGqVpPpey+dXpzzzv1iBKN/VY4
ydjgH/LBfdTsVarmmy2vtWBxwrqkFvpdhSGCvRDl/qdO/GIDJi77dmZWkh/ic90
MNk1f38gs1jrCj8lThoar17Uo9y/Q5qJIsoNPyQrJRzqFU9F3FBjiPJF
-----END CERTIFICATE-----
```

Para RIPE, utilice `whois -r -h whois.ripe.net` *2001:0DB8:7269::/48* para buscar el registro de RDAP para su rango de direcciones. Compruebe la sección `descr` para el objeto `inetnum` (rango de red) en la salida del comando. El certificado debe agregarse como un nuevo campo `descr` para el rango de direcciones.

Puede inspeccionar la sección `descr` que contiene el certificado con el siguiente comando:

```
whois -r -h whois.ripe.net 2001:0DB8:7269::/48 | grep descr | grep BEGIN
```

Esto devuelve un resultado con el contenido de la clave, que debería ser similar a lo siguiente:

```
descr:
-----BEGIN CERTIFICATE-----MIID1zCCAr+gAwIBAgIUBkRPNSLrPqbRAFP8
RDAHSP+I1TowDQYJKoZIhvcNAQELBQAwezELMAkGA1UEBhMCTloxETAPBgNVBAg
MCEF1Y2tsYW5kMREwDwYDVQQHDAhBdWNrbGFuZDEcMBoGA1UECgwTQW1hem9uIF
dlYiBTZXJ2aWNlczETMBEGA1UECwwKQllPSVAgRGVtbzETMBEGA1UEAwwKQllPS
VAgRGVtbzAeFw0yMTEyMDcyMDI0NTRaFw0yMjEyMDcyMDI0NTRaMHsxCzAJBgNV
BAYTAk5aMREwDwYDVQQIDAhBdWNrbGFuZDERMA8GA1UEBwwIQXVja2xhbmQxHDA
aBgNVBAoME0FtYXpvbiBXZWIgU2VydmljZXMxEzARBgNVBAsMCkJZT0lQIERlbW
8xEzARBgNVBAMMCkJZT0lQIERlbW8wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwg
gEKAoIBAQCfmacvDp0wZ0ceiXXcR/q27mHI/U5HKt7SST4X2eAqufR9wXkfNanA
EskgAseyFypwEEQr4CJijI/5hp9prh+jsWHWwkFRoBRR9FBtwcU/45XDXLga7D3
stsI5QesHVRwOaXUdprAnndaTugmDPkD0vrl475JWDSIm+PUxGWLy+60aBqiaZq
35wU/x+wXlAqBXg4MZK2KoUu27kYt2zhmy0S7Ky+oRfRJ9QbAiSu/RwhQbh5Mkp
1ZnVIc7NqnhdeIW48QaYjhMlUEfxdaqYUinzz8KpjfADZ4Hvqj9jWZ/eXo/9b2r
GlHWkJsbhr0VEUyAGu1bwkgcdww3A7NjOxQbAgMBAAGjUzBRMB0GA1UdDgQWBBS
tFyujN6SYBr2glHpGt0XGF7GbGTAfBgNVHSMEGDAWgBStFyujN6SYBr2glHpGt0
XGF7GbGTAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBCwUAA4IBAQBX6nn6Y
Lhz521lfyVfxY0t6o3410bQAeAF08ud+ICtmQ4IO4A4B7zV3zIVYr0clrOOaFyL
xngwMYN0XY5tVhDQqk4/gmDNEKSZy2QkX4Eg0YUWVzOyt6fPzjOvJLcsqc1hcF9
wySL507XQz76Uk5cFypBOzbnk35UkWrzA9KK97cXckfIESgK/k1N4ecwxwG6VQ8
mBGqVpPpey+dXpzzzv1iBKN/VY4ydjgH/LBfdTsVarmmy2vtWBxwrqkFvpdhSGC
vRDl/qdO/GIDJi77dmZWkh/ic90MNk1f38gs1jrCj8lThoar17Uo9y/Q5qJIsoN
PyQrJRzqFU9F3FBjiPJF
-----END CERTIFICATE-----
```

Para APNIC, utilice `whois -h whois.apnic.net` *`2001:0DB8:6170::/48`* para buscar el registro de RDAP para su rango de direcciones BYOIP. Compruebe la sección `remarks` para el objeto `inetnum` (rango de red) en la salida del comando. El certificado debe agregarse como un nuevo campo `remarks` para el rango de direcciones.

Puede inspeccionar la sección `remarks` que contiene el certificado con el siguiente comando:

```
whois -h whois.apnic.net 2001:0DB8:6170::/48 | grep remarks | grep BEGIN
```

Esto devuelve un resultado con el contenido de la clave, que debería ser similar a lo siguiente:

```
remarks:
-----BEGIN CERTIFICATE-----
```

```
MIID1zCCAr+gAwIBAgIUBkRPNSLrPqbRAFP8RDAHSP+I1TowDQYJKoZIhvcNAQE
LBQAwezELMAkGA1UEBhMCTloxETAPBgNVBAgMCEF1Y2tsYW5kMREwDwYDVQQHDA
hBdWNrbGFuZDEcMBoGA1UECgwTQW1hem9uIFdlYiBTZXJ2aWNlczETMBEGA1UEC
wwKQllPSVAgRGVtbzETMBEGA1UEAwwKQllPSVAgRGVtbzAeFw0yMTEyMDcyMDI0
NTRaFw0yMjEyMDcyMDI0NTRaMHsxCzAJBgNVBAYTAk5aMREwDwYDVQQIDAhBdWN
rbGFuZDERMA8GA1UEBwwIQXVja2xhbmQxHDAaBgNVBAoME0FtYXpvbiBXZWIgU2
VydmljZXMxEzARBgNVBAsMCkJZT0lQIERlbW8xEzARBgNVBAMMCkJZT0lQIERlb
W8wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCfmacvDp0wZ0ceiXXc
R/q27mHI/U5HKt7SST4X2eAqufR9wXkfNanAEskgAseyFypwEEQr4CJijI/5hp9
prh+jsWHWwkFRoBRR9FBtwcU/45XDXLga7D3stsI5QesHVRwOaXUdprAnndaTug
mDPkD0vrl475JWDSIm+PUxGWLy+60aBqiaZq35wU/x+wXlAqBXg4MZK2KoUu27k
Yt2zhmy0S7Ky+oRfRJ9QbAiSu/RwhQbh5Mkp1ZnVIc7NqnhdeIW48QaYjhMlUEf
xdaqYUinzz8KpjfADZ4Hvqj9jWZ/eXo/9b2rGlHWkJsbhr0VEUyAGu1bwkgcdww
3A7NjOxQbAgMBAAGjUzBRMB0GA1UdDgQWBBStFyujN6SYBr2glHpGt0XGF7GbGT
AfBgNVHSMEGDAWgBStFyujN6SYBr2glHpGt0XGF7GbGTAPBgNVHRMBAf8EBTADA
QH/MA0GCSqGSIb3DQEBCwUAA4IBAQBX6nn6YLhz521lfyVfxY0t6o3410bQAeAF
08ud+ICtmQ4IO4A4B7zV3zIVYr0clrOOaFyLxngwMYN0XY5tVhDQqk4/gmDNEKS
Zy2QkX4Eg0YUWVzOyt6fPzjOvJLcsqc1hcF9wySL507XQz76Uk5cFypBOzbnk35
UkWrzA9KK97cXckfIESgK/k1N4ecwxwG6VQ8mBGqVpPpey+dXpzzzv1iBKN/VY4
ydjgH/LBfdTsVarmmy2vtWBxwrqkFvpdhSGCvRDl/qdO/GIDJi77dmZWkh/ic90
MNk1f38gs1jrCj8lThoar17Uo9y/Q5qJIsoNPyQrJRzqFU9F3FBjiPJF
-----END CERTIFICATE-----
```

2. Validación de la creación de un objeto ROA

   Valide la creación correcta de los objetos ROA mediante la API de datos RIPEstat. Asegúrese de probar su rango de direcciones con los ASN 16509 y 14618 de Amazon, además de los ASN que cuentan actualmente con autorización para anunciar el rango de direcciones.

   Puede inspeccionar los objetos ROA desde distintos ASN de Amazon con su rango de direcciones mediante el siguiente comando:

   ```
   curl --location --request GET "https://stat.ripe.net/data/rpki-validation/data.json?
   resource=ASN&prefix=CIDR
   ```

   En este resultado de ejemplo, la respuesta tiene un resultado de `"status": "valid"` para el ASN 16509 de Amazon. Esto indica que el objeto ROA para el rango de direcciones se creó correctamente:

   ```
   {
       "messages": [],
       "see_also": [],
   ```

```
    "version": "0.3",
    "data_call_name": "rpki-validation",
    "data_call_status": "supported",
    "cached": false,
    "data": {
        "validating_roas": [
            {
                "origin": "16509",
                "prefix": "2001:0DB8::/32",
                "max_length": 48,
                "validity": "valid"
            },
            {
                "origin": "14618",
                "prefix": "2001:0DB8::/32",
                "max_length": 48,
                "validity": "invalid_asn"
            },
            {
                "origin": "64496",
                "prefix": "2001:0DB8::/32",
                "max_length": 48,
                "validity": "invalid_asn"
            }
        ],
        "status": "valid",
        "validator": "routinator",
        "resource": "16509",
        "prefix": "2001:0DB8::/32"
    },
    "query_id": "20230224152430-81e6384e-21ba-4a86-852a-31850787105f",
    "process_time": 58,
    "server_id": "app116",
    "build_version": "live.2023.2.1.142",
    "status": "ok",
    "status_code": 200,
    "time": "2023-02-24T15:24:30.773654"
}
```


El estado “unknown” indica que el objeto ROA para el rango de direcciones no se ha creado. El estado “invalid_asn” indica que el objeto ROA para el rango de direcciones no se creó correctamente.

Disponibilidad regional

La característica BYOIP está disponible actualmente en todas las regiones comerciales de AWS, excepto en las regiones de China.

Disponibilidad en la zona local

Una zona local es una extensión de una región de AWS que se encuentra geográficamente cerca de los usuarios. Las zonas locales se agrupan en “grupos fronterizos de red”. En AWS, un grupo fronterizo de red es un conjunto de zonas de disponibilidad (AZ), zonas locales o zonas de Wavelength desde las que AWS anuncia una dirección IP pública. Es posible que las zonas locales tengan grupos fronterizos de red diferentes a los de las AZ de una región de AWS para garantizar una latencia o una distancia física mínima entre la red de AWS y los clientes que acceden a los recursos de estas zonas.

Puede aprovisionar intervalos de direcciones BYOIPv4 y anunciarlos en los siguientes grupos fronterizos de red de las zonas locales mediante la opción `--network-border-group`:

- us-east-1-dfw-2
- us-west-2-lax-1
- us-west-2-phx-2

Si tiene zonas locales habilitadas (consulte Habilitar una zona local), puede elegir un grupo fronterizo de red para las zonas locales al aprovisionar y anunciar un CIDR de BYOIPv4. Elija el grupo de bordes de red con cuidado, ya que la EIP y el recurso de AWS al que está asociado deben residir en el mismo grupo de bordes de red.

> **Note**
>
> En este momento, no puede aprovisionar ni anunciar intervalos de direcciones BYOIPv6 en las zonas locales.

Más información

Para obtener más información, consulte la charla tecnológica online de AWS Deep Dive on Bring Your Own IP.

Direcciones IP elásticas

Las direcciones IP elásticas son direcciones IPv4 estáticas diseñadas para la informática en la nube dinámica. Se asigna una dirección IP elástica a su cuenta de AWS, que es suya hasta que la libere. Con una dirección IP elástica, puede enmascarar los errores de una instancia o software volviendo a mapear rápidamente la dirección a otra instancia de su cuenta. Si lo prefiere, puede especificar la dirección IP elástica en un registro DNS para el dominio, de modo que el dominio apunte a la instancia. Para obtener más información, consulte la documentación del registrador de dominios.

Una dirección IP elástica es una dirección IPv4 pública, a la que se puede tener acceso desde Internet. Si la instancia no tiene una dirección IPv4 pública, puede asociar una dirección IP elástica a la instancia para habilitar la comunicación con Internet. Por ejemplo, esto le permite conectarse a la instancia desde el equipo local.

Contenido

Precios de las direcciones IP elásticas

AWS cobra por todas las direcciones IPv4 públicas, incluidas las direcciones IPv4 públicas asociadas a las instancias en ejecución y las direcciones IP elásticas. Para obtener más información, consulte la pestaña Dirección IPv4 pública en la página Precios de Amazon VPC.

Conceptos básicos de las direcciones IP elásticas

A continuación, se describen las características básicas de una dirección IP elástica:

- Una dirección IP elástica es estática; no cambia con el tiempo.
- Una dirección IP elástica se utiliza únicamente en una región específica y no se puede mover a otra región.
- Una dirección IP elástica proviene del grupo de direcciones IPv4 de Amazon o de un grupo de direcciones IPv4 personalizado que haya llevado a su cuenta de AWS.
- Para utilizar una dirección IP elástica, primero asigne una a su cuenta y, a continuación, asóciela a su instancia o a una interfaz de red.

- Cuando asocia una dirección IP elástica a una instancia, también se asocia a la interfaz de red principal de la instancia. Cuando asocia una dirección IP elástica con una interfaz de red asociada a una instancia, también se asocia a la instancia.
- Si asocia una dirección IP elástica a una instancia o a su interfaz de red principal, la dirección IPv4 pública de la instancia (en caso de que tenga una asociada) se liberará de nuevo al grupo de direcciones IPv4 públicas de Amazon y la dirección IP elástica se asociará a la instancia en su lugar. No se puede reutilizar una dirección IPv4 pública asociada previamente a la instancia y no se puede convertir una dirección IPv4 pública en una dirección IP elástica. Para obtener más información, consulte Direcciones IPv4 públicas.
- Puede anular la asociación de una dirección IP elástica de un recurso y, a continuación, volver a asociarla a otro recurso. Para evitar comportamientos inesperados, asegúrese de que todas las conexiones activas al recurso nombrado en la asociación existente estén cerradas antes de realizar el cambio. Después de asociar la dirección IP elástica a un recurso diferente, puede volver a abrir las conexiones al recurso recién asociado.
- Una dirección IP elástica desasociada sigue asociada a su cuenta hasta que la libera explícitamente. Se le cobrará por todas las direcciones IP elásticas de su cuenta, independientemente de si están asociadas o disociadas a una instancia. Para obtener más información, consulte la pestaña Dirección IPv4 pública en la página Precios de Amazon VPC.
- Si asocia una dirección IP elástica a una instancia que anteriormente tenía una dirección IPv4 pública, el nombre de host del DNS público de la instancia cambia para que coincida con la dirección IP elástica.
- Resolvemos un nombre de host de DNS público en la dirección IPv4 pública o la dirección IP elástica de la instancia fuera de la red de la instancia y en una dirección IPv4 privada de la instancia desde dentro de la red de la instancia.
- Al asignar una dirección IP elástica desde un grupo de direcciones IP llevadas a su cuenta de AWS, esta no se incluye en el recuento del límite de direcciones IP elásticas. Para obtener más información, consulte Cuota de direcciones IP elásticas.
- Cuando asigne direcciones IP elásticas, puede asociarlas a un grupo de bordes de red. Esta es la ubicación desde la que anunciamos el bloque de CIDR. Si se establece el grupo de bordes de red, el bloque de CIDR queda restringido a este grupo. Si no se especifica el grupo de bordes de red, establecemos el grupo de bordes que contiene todas las zonas de disponibilidad de la región (por ejemplo, `us-west-2`).
- Una dirección IP elástica solo se puede utilizar para su uso en un grupo de bordes de red específico.

Trabajar con direcciones IP elásticas

En las secciones siguientes, se describe cómo se utilizan las direcciones IP elásticas.

Tareas

Asignar una dirección IP elástica

Puede asignar una dirección IP elástica desde un grupo de direcciones IPv4 públicas de Amazon o desde un grupo de direcciones IP personalizado que haya llevado a su cuenta de AWS. Para obtener más información acerca de llevar su rango de direcciones IP a su cuenta de AWS, consulte Traiga sus propias direcciones IP (BYOIP) en Amazon EC2.

Puede asignar una dirección IP elástica mediante uno de los métodos siguientes.

Console

Para asignar una dirección IP elástica

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Red y seguridad, IP elásticas.
3. Elija Asignar dirección IP elástica.
4. (Opcional) Si asigna una dirección IP elástica (EIP), elija el Grupo de bordes de red al que desea asignar la EIP. Un grupo de bordes de red es un conjunto de zonas de disponibilidad (AZ), zonas locales o zonas de Wavelength desde las que AWS anuncia una dirección IP pública. Es posible que las zonas locales y las zonas de Wavelength tengan grupos de bordes de red diferentes a los de las AZ de una región para garantizar una latencia o una

distancia física mínima entre la red de AWS y los clientes que acceden a los recursos de estas zonas.

> **Important**
>
> Debe asignar una EIP en el mismo grupo de bordes de red que el recurso de AWS que se asociará a la EIP. Una EIP de un grupo de bordes de red solo se puede anunciar en zonas de ese grupo de bordes de red y no en otras zonas representadas por otros grupos de bordes de red.

Si tiene zonas locales o zonas de Wavelength habilitadas (para obtener más información, consulte Habilitar una zona local o Habilitar zonas de Wavelength), puede elegir un grupo de bordes de red para las AZ, las zonas locales o las zonas de Wavelength. Elija el grupo de bordes de red con cuidado, ya que la EIP y el recurso de AWS al que está asociado deben residir en el mismo grupo de bordes de red. Puede utilizar la consola de EC2 para ver el grupo de bordes de red en el que se encuentran las zonas de disponibilidad, las zonas locales o las zonas de Wavelength. Por lo general, todas las zonas de disponibilidad de una región pertenecen al mismo grupo de bordes de red, mientras que las zonas locales o las zonas de Wavelength pertenecen a sus propios grupos de bordes de red independientes.

Si las zonas locales o las zonas de Wavelength no están habilitadas, cuando asigna una EIP, el grupo de bordes de red que representa a todas las AZ de la región (por ejemplo `us-west-2`) se predefine para usted y no puede cambiarlo. Esto significa que la EIP que asigne a este grupo de bordes de red se anunciará en todas las zonas de disponibilidad de la región en la que usted se encuentre.

5. En Grupo de direcciones IPv4 públicas, elija una de las siguientes opciones:

   - Grupo de direcciones IPv4 de Amazon: si desea que una dirección IPv4 se asigne desde un grupo de direcciones IPv4 de Amazon.
   - Direcciones IPv4 públicas que trae a su cuenta de AWS: si desea asignar una dirección IPv4 de un grupo de direcciones IP que trajo a su cuenta de AWS. Esta opción está deshabilitada si no tiene grupos de direcciones IP.
   - Grupo de direcciones IPv4 propiedad del cliente: si desea asignar una dirección IPv4 de un grupo creado desde la red en las instalaciones para su uso con un AWS Outpost. Esta opción está desactivada si no tiene un Outpost de AWS.

6. (Opcional) Añada o elimine una etiqueta.

[Agregar una etiqueta] Elija Agregar nueva etiqueta y haga lo siguiente:

- En Clave, escriba el nombre de la clave.
- En Valor, escriba el valor de la clave.

[Eliminar una etiqueta] Elija Eliminar a la derecha de la clave y el valor de la etiqueta.

7. Elija Asignar.

AWS CLI

Para asignar una dirección IP elástica

Utilice el comando allocate-address de la AWS CLI.

PowerShell

Para asignar una dirección IP elástica

Utilice el comando New-EC2Address de AWS Tools for Windows PowerShell.

Describir las direcciones IP elásticas

Puede describir una dirección IP elástica mediante uno de los métodos siguientes.

Console

Para describir sus direcciones IP elásticas

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Elastic IPs (Direcciones IP elásticas).
3. Seleccione la dirección IP elástica que desea ver y elija Acciones, Ver detalles.

AWS CLI

Para describir sus direcciones IP elásticas

Utilice el comando describe-addresses de la AWS CLI.

PowerShell

Para describir sus direcciones IP elásticas

Utilice el comando Get-EC2Address de AWS Tools for Windows PowerShell.

Etiquetado de una dirección IP elástica

Puede asignar etiquetas personalizadas a sus direcciones IP elásticas para clasificarlas de diversas maneras; por ejemplo, por finalidad, propietario o entorno. Esto ayuda a buscar rápidamente una dirección IP elástica específica según las etiquetas personalizadas que le haya asignado.

No se admite el seguimiento de asignación de costos utilizando etiquetas de direcciones IP elásticas.

Puede etiquetar una dirección IP elástica mediante uno de los métodos siguientes.

Console

Para etiquetar una dirección IP elástica

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Elastic IPs (Direcciones IP elásticas).
3. Seleccione la dirección IP elástica que desea etiquetar y elija Acciones, Ver detalles.
4. En la sección Etiquetas, elija Administrar etiquetas.
5. Especificar una clave de etiqueta y un par de valor.
6. (Opcional) Elija Agregar etiqueta para agregar etiquetas adicionales.
7. Seleccione Guardar.

AWS CLI

Para etiquetar una dirección IP elástica

Utilice el comando create-tags de la AWS CLI.

```
aws ec2 create-tags --resources eipalloc-12345678 --tags Key=Owner,Value=TeamA
```

PowerShell

Para etiquetar una dirección IP elástica

Utilice el comando New-EC2Tag de AWS Tools for Windows PowerShell.

El comando `New-EC2Tag` necesita un parámetro `Tag`, que especifica el par de clave y valor que se va a utilizar para la etiqueta de la dirección IP elástica. Los siguientes comandos crean el parámetro `Tag`.

```
PS C:\> $tag = New-Object Amazon.EC2.Model.Tag
 PS C:\> $tag.Key = "Owner"
 PS C:\> $tag.Value = "TeamA"
```

```
PS C:\> New-EC2Tag -Resource eipalloc-12345678 -Tag $tag
```

Asociación de una dirección IP elástica a una instancia o una interfaz de red

Si va a asociar una dirección IP elástica a la instancia para permitir la comunicación con Internet, también debe asegurarse de que la instancia esté en una subred pública. Para obtener más información, consulte Puertas de enlace de Internet en la Guía del usuario de Amazon VPC.

Puede asociar una dirección IP elástica a una instancia o interfaz de red mediante uno de los métodos siguientes.

Console

Para asociar una dirección IP elástica a una instancia

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Elastic IPs (Direcciones IP elásticas).
3. Seleccione la dirección IP elástica que desea asociar y elija Acciones, Asociar dirección IP elástica.
4. En Tipo de recurso, elija Instancia.
5. Por ejemplo, elija la instancia con la que asociar la dirección IP elástica. También puede escribir texto para buscar una instancia específica.
6. (Opcional) En Dirección IP privada, especifique una dirección IP privada a la que asociar la dirección IP elástica.
7. Elija Associate.

Para asociar una dirección IP elástica a una interfaz de red

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Elastic IPs (Direcciones IP elásticas).
3. Seleccione la dirección IP elástica que desea asociar y elija Acciones, Asociar dirección IP elástica.
4. En Tipo de recurso, elija Interfaz de red.
5. En Interfaz de red, elija la interfaz de red con la que asociar la dirección IP elástica. También puede escribir texto para buscar una interfaz de red específica.
6. (Optional) En Private IP address (Dirección IP privada), especifique una dirección IP privada con la que asociar la dirección IP elástica.
7. Elija Associate.

AWS CLI

Para asociar una dirección IP elástica

Utilice el comando associate-address de la AWS CLI.

PowerShell

Para asociar una dirección IP elástica

Utilice el comando Register-EC2Address de AWS Tools for Windows PowerShell.

Anulación de la asociación de una dirección IP elástica

Puede anular la asociación de una dirección IP elástica de una instancia o interfaz de red en cualquier momento. Después de anular la asociación de la dirección IP elástica, puede volver a asociarla con otro recurso.

Puede anular la asociación de una dirección IP elástica mediante uno de los métodos siguientes.

Console

Para anular la asociación y volver a asociar una dirección IP elástica

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Elastic IPs (Direcciones IP elásticas).

3. Seleccione la dirección IP elástica cuya asociación desea anular, elija Acciones, Anular la asociación de la dirección IP elástica.
4. Elija Desasociar.

AWS CLI

Para anular la asociación de una dirección IP elástica

Utilice el comando disassociate-address de la AWS CLI.

PowerShell

Para anular la asociación de una dirección IP elástica

Utilice el comando Unregister-EC2Address de AWS Tools for Windows PowerShell.

Transferencia de las direcciones IP elásticas

En esta sección se describe cómo transferir las direcciones IP elásticas de una Cuenta de AWS a otra. La transferencia de direcciones IP elásticas puede resultar útil en las siguientes situaciones:

- Reestructuración organizativa: utilice las transferencias de direcciones IP elásticas para mover rápidamente las cargas de trabajo de una Cuenta de AWS a otra. No debe esperar a que se permita incluir nuevas direcciones IP elásticas en sus grupos de seguridad y NACL.
- Administración de seguridad centralizada: utilice una cuenta de seguridad de AWS centralizada para rastrear y transferir direcciones IP elásticas que se hayan examinado y cumplan con las normas de seguridad.
- Recuperación de desastres: utilice las transferencias de direcciones IP elásticas para reasignar rápidamente las IP a las cargas de trabajo de Internet orientadas al público durante eventos de emergencia.

La transferencia de direcciones IP elásticas no implica cargos.

Tareas

- Habilitar la transferencia de direcciones IP elásticas
- Deshabilitar la transferencia de direcciones IP elásticas
- Aceptar una dirección IP elástica transferida

Habilitar la transferencia de direcciones IP elásticas

En esta sección, se describe cómo aceptar una dirección IP elástica que se ha transferido. Tenga en cuenta las siguientes limitaciones relacionadas con la habilitación de direcciones IP elásticas para su transferencia:

- Puede transferir direcciones IP elásticas de cualquier Cuenta de AWS (cuenta de origen) a cualquier otra cuenta de AWS de la misma región de AWS (cuenta de transferencia).
- Al transferir una dirección IP elástica, hay un protocolo de enlace de dos pasos entre Cuentas de AWS. Cuando la cuenta de origen inicie la transferencia, las cuentas de transferencia tienen siete días para aceptar la transferencia de la dirección IP elástica. Durante esos siete días, la cuenta de origen puede ver la transferencia pendiente (por ejemplo, en la consola de AWS o mediante el comando de la AWS CLI describe-address-transfers). Transcurridos siete días, la transferencia caduca y la propiedad de la dirección IP elástica vuelve a la cuenta de origen.
- Las transferencias aceptadas están visibles en la cuenta de origen (por ejemplo, en laAWS consola o mediante elAWS CLI comando describe-address-transfers) durante tres días después de que se hayan aceptado las transferencias.
- AWS no notifica a las cuentas de transferencia sobre las solicitudes pendientes de transferencia de direcciones IP elásticas. El propietario de la cuenta de origen debe notificar al propietario de la cuenta de transferencia que hay una solicitud de transferencia de direcciones IP elásticas que debe aceptar.
- Todas las etiquetas asociadas a la dirección IP elástica que se transfiere se restablecen cuando se completa la transferencia.
- No puede transferir las direcciones IP elásticas asignadas desde los grupos de direcciones IPv4 públicas que incorpore a su Cuenta de AWS (normalmente denominados grupos de direcciones traiga su propia IP [BYOIP]).
- Si intenta transferir una dirección IP elástica que tenga un registro DNS inverso asociado, puede iniciar el proceso de transferencia, pero la cuenta de transferencia no podrá aceptar la transferencia hasta que se elimine el registro DNS asociado.
- Si ha habilitado y configurado AWS Outposts, es posible que haya asignado direcciones IP elásticas de un grupo de direcciones IP (CoIP) que son propiedad del cliente. No puede transferir direcciones IP elásticas asignadas desde una CoIP. Sin embargo, puede usar AWS RAM para compartir un CoIP con otra cuenta. Para obtener más información, consulte Direcciones IP propiedad del cliente en la Guía del usuario de AWS Outposts.
- Puede utilizar Amazon VPC IPAM para hacer un seguimiento de la transferencia de direcciones IP elásticas a cuentas de una organización desde AWS Organizations. Para obtener más información,

consulte Ver historial de direcciones IP. Si se transfiere una dirección IP elástica a una Cuenta de AWS fuera de la organización, se pierde el historial de auditoría de IPAM de la dirección IP elástica.

La cuenta de origen debe completar estos pasos.

Console

Para habilitar la transferencia de direcciones IP elásticas

1. Asegúrese de utilizar la cuenta de AWS de origen.
2. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
3. En el panel de navegación, elija Direcciones IP elásticas.
4. Seleccione una o más direcciones IP elásticas para habilitar la transferencia y elija Acciones, Habilitar la transferencia.
5. Si está transfiriendo varias direcciones IP elásticas, verá la opción Tipo de transferencia. Seleccione una de las siguientes opciones:
   - Elija Una sola cuenta si va a transferir las direcciones IP elásticas a una sola cuenta de AWS.
   - Elija Varias cuentas si va a transferir las direcciones IP elásticas a varias cuentas de AWS.
6. En Transferir ID de cuenta, ingrese los ID de las cuentas de AWS a las que quiere transferir las direcciones IP elásticas.
7. Para confirmar la transferencia, ingrese **`enable`** en el cuadro de texto.
8. Seleccione Submit (Enviar).
9. Para aceptar la transferencia, consulte Aceptar una dirección IP elástica transferida.
   Para deshabilitar la transferencia, consulte Deshabilitar la transferencia de direcciones IP elásticas.

AWS CLI

Para habilitar la transferencia de direcciones IP elásticas

Utilice el comando enable-address-transfer.

PowerShell

Para habilitar la transferencia de direcciones IP elásticas

Utilice el comando Enable-EC2AddressTransfer.

Deshabilitar la transferencia de direcciones IP elásticas

En esta sección, se describe cómo deshabilitar una transferencia de una dirección IP elástica una vez se ha habilitado la transferencia.

La cuenta de origen que habilitó la transferencia debe llevar a cabo estos pasos.

Console

Para deshabilitar la transferencia de una dirección IP elástica

1. Asegúrese de utilizar la cuenta de AWS de origen.
2. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
3. En el panel de navegación, elija Elastic IPs (Direcciones IP elásticas).
4. En la lista de recursos de IP elásticas, asegúrese de tener habilitada la propiedad que muestra la columna Estado de la transferencia.
5. Seleccione una o más direcciones IP elásticas que tengan un Estado de la transferencia en Pendiente y elija Acciones, Deshabilitar la transferencia.
6. Para confirmarlo, ingrese **`disable`** en el cuadro de texto.
7. Seleccione Submit (Enviar).

AWS CLI

Para deshabilitar la transferencia de direcciones IP elásticas

Utilice el comando disable-address-transfer.

PowerShell

Para deshabilitar la transferencia de direcciones IP elásticas

Utilice el comando Disable-EC2AddressTransfer.

Aceptar una dirección IP elástica transferida

En esta sección, se describe cómo aceptar una dirección IP elástica que se ha transferido.

Al transferir una dirección IP elástica, hay un protocolo de enlace de dos pasos entre Cuentas de AWS. Cuando la cuenta de origen inicie la transferencia, las cuentas de transferencia tienen siete días para aceptar la transferencia de la dirección IP elástica. Durante esos siete días, la cuenta de origen puede ver la transferencia pendiente (por ejemplo, en la consola de AWS o mediante el comando de la AWS CLI describe-address-transfers). Transcurridos siete días, la transferencia caduca y la propiedad de la dirección IP elástica vuelve a la cuenta de origen.

Al aceptar las transferencias, tenga en cuenta las siguientes excepciones que pueden tener lugar y cómo solucionarlas:

- AddressLimitExceed: si su cuenta de transferencia superó la cuota de direcciones IP elásticas, la cuenta de origen puede habilitar la transferencia de direcciones IP elásticas, pero esta excepción se produce cuando la cuenta de transferencia intenta aceptarla. De forma predeterminada, todas las cuentas de AWS están limitadas a cinco (5) direcciones IP elásticas por región. Consulte Cuota de direcciones IP elásticas para obtener instrucciones sobre cómo aumentar el límite.
- InvalidTransfer.AddressCustomPtrset: si usted o alguien de su organización ha configurado la dirección IP elástica que intenta transferir para utilizar la búsqueda de DNS inversa, la cuenta de origen puede habilitar la transferencia de la dirección IP elástica, pero esta excepción se produce cuando la cuenta de transferencia intenta aceptarla. Para resolver este problema, la cuenta de origen debe eliminar el registro de DNS de la dirección IP elástica. Para obtener más información, consulte Usar DNS inverso para aplicaciones de correo electrónico.
- InvalidTransfer.AddressAssociated: si una dirección IP elástica está asociada a una instancia de ENI o EC2, la cuenta de origen puede habilitar la transferencia de la dirección IP elástica, pero esta excepción se produce cuando la cuenta de transferencia intenta aceptarla. Para resolver este problema, la cuenta de origen debe desasociar la dirección IP elástica. Para obtener más información, consulte Anulación de la asociación de una dirección IP elástica.

Para otras excepciones, contacte con AWS Support.

La cuenta de transferencia debe completar estos pasos.

Console

Para aceptar la transferencia de una dirección IP elástica

1. Asegúrese de utilizar la cuenta de transferencia.
2. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
3. En el panel de navegación, elija Elastic IP.

4. Elija Acciones, Aceptar la transferencia.
5. No se transfiere ninguna etiqueta asociada a la dirección IP elástica que se transfiere con la dirección IP elástica cuando acepta la transferencia. Si desea definir una etiqueta Nombre de la dirección IP elástica que acepta, seleccione Crear una etiqueta con la clave “Nombre” y un valor que especifique.
6. Ingrese la dirección IP elástica que quiere transferir.
7. Si acepta la transferencia de varias direcciones IP elásticas, elija Agregar dirección para ingresar una dirección IP elástica adicional.
8. Seleccione Submit (Enviar).

AWS CLI

Para aceptar la transferencia de una dirección IP elástica

Utilice el comando accept-address-transfer.

PowerShell

Para aceptar la transferencia de una dirección IP elástica

Utilice el comando Approve-EC2AddressTransfer.

Liberación de una dirección IP elástica

Si ya no necesita una dirección IP elástica, le recomendamos que la libere mediante uno de los métodos siguientes. La dirección que se va a publicar no debe estar asociada actualmente a un recurso de AWS, como una instancia de EC2, una puerta de enlace NAT o un equilibrador de carga de red.

> **Note**
>
> Si se puso en contacto con AWS Support para configurar un DNS inverso para una dirección IP elástica (EIP), puede eliminar el DNS inverso, pero no puede iniciar la dirección IP elástica porque AWS Support la bloqueó. Para desbloquear la dirección IP elástica, contáctese con AWS Support. Una vez desbloqueada, podrá liberar la dirección IP elástica.

Console

Para liberar una dirección IP elástica

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Elastic IPs (Direcciones IP elásticas).
3. Seleccione la dirección IP elástica que desea liberar y elija Acciones, Liberar direcciones IP elásticas.
4. Elija Liberar.

AWS CLI

Para liberar una dirección IP elástica

Utilice el comando release-address de la AWS CLI.

PowerShell

Para liberar una dirección IP elástica

Utilice el comando Remove-EC2Address de AWS Tools for Windows PowerShell.

Recuperar una dirección IP elástica

Si ha liberado su dirección IP elástica, es posible recuperarla. Se aplican las siguientes reglas:

- No puede recuperar una dirección IP elástica si se ha asignado a otra cuenta de AWS o si al hacerlo superará el límite de direcciones IP elásticas.
- No es posible recuperar etiquetas asociadas con una dirección IP elástica.
- Únicamente puede recuperar una dirección IP elástica con la API de Amazon EC2 o con una herramienta de la línea de comandos.

AWS CLI

Para recuperar una dirección IP elástica

Utilice el comando allocate-address de la AWS CLI y especifique la dirección IP mediante el parámetro `--address` como se indica a continuación.

```
aws ec2 allocate-address --domain vpc --address 203.0.113.3
```

PowerShell

Para recuperar una dirección IP elástica

Utilice el comando New-EC2Address de AWS Tools for Windows PowerShell y especifique la dirección IP mediante el parámetro `-Address` como se indica a continuación.

```
PS C:\> New-EC2Address -Address 203.0.113.3 -Domain vpc -Region us-east-1
```

Usar DNS inverso para aplicaciones de correo electrónico

Si desea enviar correo electrónico a terceros desde una instancia, le recomendamos aprovisionar una o más direcciones IP elásticas y asignar registros DNS inversos estáticos a las direcciones IP elásticas que utilice para enviar correo electrónico. Esto lo ayuda a evitar que algunas organizaciones antispam marquen su email como spam. AWS trabaja con ISP y organizaciones antispam de Internet para reducir las posibilidades de que sus emails que se envían desde estas direcciones se marquen como spam.

Consideraciones

- Antes de crear un registro DNS inverso, debe establecer un registro DNS de reenvío correspondiente (tipo de registro A) que apunte a la dirección IP elástica.
- Si hay asociado un registro de DNS inverso a una dirección IP elástica, esa dirección se bloquea en la cuenta y no se puede liberar hasta que se elimine el registro.
- AWS GovCloud (US) Region

  No puede crear un registro DNS inverso con los métodos por medio de la consola o AWS CLI. AWS debe asignar los registros DNS inversos estáticos en su nombre. Abra Solicitud para eliminar las limitaciones de envío de email y DNS inverso y proporcione sus direcciones IP elásticas y los registros de DNS inversos.

Crear un registro de DNS inverso

Para crear un registro DNS inverso, elija la pestaña que coincida con su método preferido.

Console

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Elastic IPs (Direcciones IP elásticas).
3. Seleccione la dirección IP elástica y elija Acciones, Actualizar DNS inverso.
4. Para Nombre de dominio de DNS inverso, escriba el nombre de su dominio.
5. Escriba **update** para confirmar.
6. Elija Actualizar.

AWS CLI

Utilice el comando modify-address-attribute en AWS CLI tal y como se muestra en el siguiente ejemplo:

```
aws ec2 modify-address-attribute --allocation-id eipalloc-abcdef01234567890  --
domain-name example.com
{
    "Addresses": [
        {
            "PublicIp": "192.0.2.0",
            "AllocationId": "eipalloc-abcdef01234567890",
            "PtrRecord": "example.net."
            "PtrRecordUpdate": {
                "Value": "example.com.",
                "Status": "PENDING"
        }
    ]
}
```

Eliminación de un registro de DNS inverso

Para eliminar un registro DNS inverso, elija la pestaña que coincida con el método que prefiera.

Console

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Elastic IPs (Direcciones IP elásticas).
3. Seleccione la dirección IP elástica y elija Acciones, Actualizar DNS inverso.

4. Para Nombre de dominio de DNS inverso, elimine el nombre de dominio.
5. Escriba **`update`** para confirmar.
6. Elija Actualizar.

AWS CLI

Utilice el comando reset-address-attribute en AWS CLI tal y como se muestra en el siguiente ejemplo:

```
aws ec2 reset-address-attribute --allocation-id eipalloc-abcdef01234567890 --
attribute domain-name
{
    "Addresses": [
        {
            "PublicIp": "192.0.2.0",
            "AllocationId": "eipalloc-abcdef01234567890",
            "PtrRecord": "example.com."
            "PtrRecordUpdate": {
                "Value": "example.net.",
                "Status": "PENDING"
        }
    ]
}
```

> **Note**
>
> Si aparece el siguiente error al ejecutar el comando, puede enviar una Solicitud para eliminar los límites de envío de correos electrónicos para AWS Support asistencia.
> La dirección con identificador de asignación no se puede publicar porque está bloqueada en su cuenta.

Cuota de direcciones IP elásticas

De manera predeterminada, todas las cuentas de AWS tienen una cuota de cinco (5) direcciones IP elásticas por región, porque las direcciones públicas de Internet (IPv4) son un recurso público escaso. Es absolutamente recomendable que utilice una dirección IP elástica principalmente para poder reasignar la dirección a otra instancia en caso de que genere un error y utilizar nombres de host DNS para toda la comunicación entre nodos restante.

Para comprobar cuántas direcciones IP elásticas están en uso

Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/ y elija Direcciones IP elásticas en el panel de navegación.

Para verificar la cuota de cuenta actual para direcciones IP elásticas

1. Abra la consola de Service Quotas en https://console.aws.amazon.com/servicequotas/.
2. Desde la barra de navegación (parte superior de la pantalla), seleccione una región.
3. En el panel, seleccione Amazon Elastic Compute Cloud (Amazon EC2).

   Si Amazon Elastic Compute Cloud (Amazon EC2) no aparece en el panel, elija Servicios de AWS, ingrese **EC2** en el campo de búsqueda y, a continuación, elija Amazon Elastic Compute Cloud (Amazon EC2).
4. En la página de cuotas de servicio de Amazon EC2, escriba **IP** en el campo de búsqueda. El límite es IP elásticas de EC2-VPC. Para obtener más información, seleccione el límite.

Si cree que su arquitectura garantiza direcciones IP elásticas adicionales, puede solicitar un aumento de cuota directamente desde la consola de Service Quotas. Para solicitar un aumento de cuota, elija Solicitud de aumento a nivel de cuenta. Para obtener más información, consulte Cuotas de servicio de Amazon EC2.

Interfaces de red elásticas

Una interfaz de red elástica es un componente de red lógico en una VPC que representa una tarjeta de red virtual. Puede incluir los siguientes atributos:

- Una dirección IPv4 privada principal del intervalo de direcciones IPv4 de la VPC
- Una dirección IPv6 privada principal del intervalo de direcciones IPv6 de la VPC
- Una o más direcciones IPv4 privada secundaria del intervalo de direcciones IPv4 de la VPC
- Una dirección IP elástica (IPv4) por dirección IPv4 privada
- Una dirección IPv4 pública
- Una o varias direcciones IPv6
- Uno o varios grupos de seguridad
- Una dirección MAC

- Una marca de comprobación de origen/destino
- Una descripción

Puede crear y configurar interfaces de red y adjuntarlas a instancias de la misma zona de disponibilidad. Su cuenta también podría tener interfaces de red administradas por el solicitante, que son creadas y administradas por los servicios de AWS para permitirle usar otros recursos y servicios. No puede administrar estas interfaces de red usted mismo. Para obtener más información, consulte Interfaces de red administradas por el solicitante.

Este recurso de AWS se denomina interfaz de red en la AWS Management Console y la API de Amazon EC2. Por lo tanto, usamos “interfaz de red” en esta documentación en lugar de “interfaz de red elástica”. El término “interfaz de red” en esta documentación siempre significa “interfaz de red elástica”.

Contenido

Conceptos básicos de interfaz de red

Puede crear una interfaz de red, conectarla a una instancia, desconectarla de una instancia y conectarla a otra instancia. Los atributos de una interfaz de red le siguen cuando se conecta o se desconecta de una instancia y se vuelve a conectar a otra instancia. Cuando mueve una interfaz de red de una instancia a otra, el tráfico de la red se redirige a la nueva instancia.

Interfaz de red principal

Cada instancia tiene una interfaz de red predeterminada denominada interfaz de red principal. No se puede desconectar una interfaz de red principal de una instancia. Puede crear y conectar interfaces de red adicionales. El número máximo de interfaces de red que puede utilizar varía en función del

tipo de instancia. Para obtener más información, consulte Direcciones IP por interfaz de red por tipo de instancia.

Direcciones IPv4 públicas para interfaces de red

En una VPC, todas las subredes tienen un atributo modificable que determina si las interfaces de red creadas en dicha subred (y, por tanto, las instancias iniciadas en ella) se asignan a una dirección IPv4 pública. Para obtener más información, consulte Configuración de subred en la Guía del usuario de Amazon VPC. La dirección IPv4 se asigna desde el grupo de direcciones IPv4 públicas de Amazon. Cuando inicia una instancia, la dirección IP se asigna a la interfaz de red principal que se crea.

Cuando crea una interfaz de red, hereda el atributo de dirección IPv4 pública de la subred. Si posteriormente modifica el atributo de dirección IPv4 pública de la subred, la interfaz de red mantiene la configuración activa cuando se creó. Si inicia una instancia y especifica una interfaz de red existente como interfaz de red principal, esta interfaz de red determina el atributo de dirección IPv4 pública.

Para obtener más información, consulte Direcciones IPv4 públicas.

Direcciones IP elásticas de la interfaz de red

Si tiene una dirección IP elástica, puede asociarla con una de las direcciones IPv4 privadas de la interfaz de red. Puede asociar una dirección IP elástica con cada dirección IPv4 privada.

Si desasocia una dirección IP elástica de una interfaz de red, puede publicarla de nuevo en el grupo de direcciones. Esta es la única forma de asociar una dirección IP elástica con una instancia de otra subred o VPC, ya que las interfaces de red son específicas de las subredes.

Direcciones IPv6 públicas para interfaces de red

Si asocia bloques de CIDR IPv6 con una VPC y una subred, puede asignar una o varias direcciones IPv6 del intervalo de la subred a una interfaz de red. Cada dirección IPv6 se puede asignar a una sola interfaz de red.

Todas las subredes tienen un atributo modificable que determina si las interfaces de red creadas en dicha subred (y, por tanto, las instancias iniciadas en dicha subred) se asignan automáticamente a una dirección IPv6 del rango de la subred. Para obtener más información, consulte Configuración de subred en la Guía del usuario de Amazon VPC. Cuando inicia una instancia, la dirección IPv6 se asigna a la interfaz de red principal que se crea.

Para obtener más información, consulte Direcciones IPv6.

Delegación de prefijos

Un prefijo de delegación de prefijo es un intervalo CIDR IPv4 o IPv6 privado reservado que se asigna para la asignación automática o manual a interfaces de red asociadas a una instancia. Si utiliza Prefijos delegados, puede iniciar servicios más rápidamente al asignar un rango de direcciones IP como un prefijo único.

Comportamiento de la terminación

Puede definir el comportamiento de terminación de una interfaz de red conecta a una instancia. Puede especificar si la interfaz de red se debe eliminar automáticamente cuando termina la instancia a la que está conectada.

Comprobación de origen/destino

Puede habilitar o deshabilitar las comprobaciones de origen/destino, que garantizan que la instancia sea el origen o el destino de cualquier tráfico que reciba. Las comprobaciones de origen/destino están habilitadas de forma predeterminada. Debe deshabilitar las comprobaciones de origen/destino si la instancia ejecuta servicios tales como la traducción o el direccionamiento de direcciones de red, o firewalls.

Monitoreo del tráfico IP

Puede habilitar un registro del flujo de VPC en la interfaz de red para capturar información acerca del tráfico IP que entra y sale de la interfaz de red. Una vez creado un registro del flujo, puede verlo y recuperar sus datos en Amazon CloudWatch Logs. Para obtener más información, consulte Registros de flujo de VPC en la Guía del usuario de Amazon VPC.

Asignación automática de direcciones IPv4 públicas

Puede habilitar o deshabilitar la asignación automática de una dirección IPv4 pública a la interfaz de red. Esta opción puede habilitarse para cualquier interfaz de red, pero solo se aplicará a la interfaz de red principal (eth0). Para obtener más información, consulte Administrar direcciones IP.

Tarjetas de red

Las instancias con varias tarjetas de red proporcionan un mayor rendimiento de red, incluidas capacidades de ancho de banda superiores a 100 Gbps y rendimiento de velocidad de paquetes

mejorado. Cada interfaz de red está conectada a una tarjeta de red. La interfaz de red principal debe asignarse al índice 0 de la tarjeta de red.

Si habilita Elastic Fabric Adapter (EFA) cuando inicia una instancia que admite varias tarjetas de red, todas las tarjetas de red estarán disponibles. Puede asignar hasta un EFA por tarjeta de red. Un EFA cuenta como una interfaz de red.

Las siguientes instancias admiten varias tarjetas de red. Todos los demás tipos de instancia admiten una tarjeta de red.

Tipo de instancia	Número de tarjetas de red
c6in.32xlarge	2
c6in.metal	2.
dl1.24xlarge	4
hpc6id.32xlarge	2
hpc7a.12xlarge	2
hpc7a.24xlarge	2
hpc7a.48xlarge	2
hpc7a.96xlarge	2
m6idn.32xlarge	2
m6idn.metal	2
m6in.32xlarge	2
m6in.metal	2.
p4d.24xlarge	4
p4de.24xlarge	4
p5.48xlarge	32

Tipo de instancia	Número de tarjetas de red
r6idn.32xlarge	2
r6idn.metal	2
r6in.32xlarge	2
r6in.metal	2.
trn1.32xlarge	8
trn1n.32xlarge	16
u7in-16tb.224xlarge	2
u7in-24tb.224xlarge	2
u7in-32tb.224xlarge	2.

Direcciones IP por interfaz de red por tipo de instancia

Cada tipo de instancia admite un número máximo de interfaces de red, un número máximo de direcciones IPv4 privadas por interfaz de red y un número máximo de direcciones IPv6 por interfaz de red. El límite de direcciones IPv6 es independiente del límite de direcciones IPv4 privadas por interfaz de red. No todos los tipos de instancias admiten las direcciones IPv6.

Interfaces de red disponibles

La Guía de tipos de instancia de Amazon EC2 proporciona información acerca de las interfaces de red disponibles para cada tipo de instancia. Para más información, consulte los siguientes temas:

- Especificaciones de red: uso general
- Especificaciones de red: optimizadas para computación
- Especificaciones de red: memoria optimizada
- Especificaciones de red: almacenamiento optimizado
- Especificaciones de red: computación acelerada
- Especificaciones de red: computación de alto rendimiento

- Especificaciones de red: generación anterior

Cómo recuperar información de la interfaz de red mediante la AWS CLI

Puede utilizar el comando de la AWS CLI describe-instance-types para mostrar información sobre un tipo de instancia, como las interfaces de red compatibles y las direcciones IP por interfaz. En el siguiente ejemplo se muestra esta información para todas las instancias C5.

```
aws ec2 describe-instance-types --filters "Name=instance-type,Values=c5.*" --query
 "InstanceTypes[].{Type: InstanceType, MaxENI: NetworkInfo.MaximumNetworkInterfaces,
 IPv4addr: NetworkInfo.Ipv4AddressesPerInterface}" --output table
-------------------------------------
|        DescribeInstanceTypes        |
+----------+----------+---------------+
| IPv4addr | MaxENI   |     Type      |
+----------+----------+---------------+
|  30      |  8       |  c5.4xlarge   |
|  50      |  15      |  c5.24xlarge  |
|  15      |  4       |  c5.xlarge    |
|  30      |  8       |  c5.12xlarge  |
|  10      |  3       |  c5.large     |
|  15      |  4       |  c5.2xlarge   |
|  50      |  15      |  c5.metal     |
|  30      |  8       |  c5.9xlarge   |
|  50      |  15      |  c5.18xlarge  |
+----------+----------+---------------+
```

Trabajar con interfaces de red

Puede trabajar con interfaces de red mediante la línea de comandos o la consola de Amazon EC2.

Contenido

- Crear una interfaz de red
- Ver detalles sobre una interfaz de red
- Asociar una interfaz de red a una instancia
- Desasociar una interfaz de red de una instancia
- Administrar direcciones IP
- Modificar atributos de interfaz de red
- Agregar o editar etiquetas

- Eliminar una interfaz de red

Crear una interfaz de red

Puede crear una interfaz de red en una subred. Una vez creada, no puede mover la interfaz de red a otra subred. Debe adjuntar una interfaz de red a una instancia de la misma zona de disponibilidad.

Para crear un interfaz de red con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Network Interfaces.
3. Elija Crear interfaz de red.
4. (Opcional) En Descripción, escriba un nombre descriptivo.
5. En Subred, seleccione una subred. Las opciones disponibles en los pasos siguientes cambian según el tipo de subred que seleccione (solo IPv4, solo IPv6 o doble pila [IPv4 e IPv6]).
6. En Dirección IPv4 privada, realice alguna de las siguientes operaciones:
   - Elija Asignación automática para permitir que Amazon EC2 seleccione una dirección IPv4 de la subred.
   - Elija Personalizado e introduzca una dirección IPv4 que seleccione de la subred.
7. (Subredes solo con direcciones IPv6) En Dirección IPv6, realice una de las siguientes operaciones:
   - Elija Ninguna si no desea asignar una dirección IPv6 a la interfaz de red.
   - Elija Asignación automática para permitir que Amazon EC2 seleccione una dirección IPv6 de la subred.
   - Elija Personalizado e introduzca una dirección IPv6 que seleccione de la subred.
8. (Opcional) Si está creando una interfaz de red en una subred de doble pila o solo para IPv6, tiene la opción de asignar la IP IPv6 principal. Esto asigna una dirección de unidifusión global (GUA) IPv6 principal a la interfaz de red. La asignación de una dirección IPv6 principal le permite evitar interrumpir el tráfico a las instancias o ENI. Escoja Habilitar si la instancia a la que se adjuntará este ENI depende de que su dirección IPv6 no cambie. AWS asignará automáticamente una dirección IPv6 asociada al ENI adjunto a la instancia como la dirección IPv6 principal. Una vez que habilite una dirección GUA de IPv6 para que sea la IPv6 principal, no podrá deshabilitarla. Al habilitar una dirección GUA de IPv6 para que sea una de IPv6 principal, la primera dirección GUA de IPv6 pasará a ser la dirección IPv6 principal hasta que se termine la instancia o se separe la interfaz de red. Si tiene varias direcciones IPv6 asociadas a

un ENI adjunto a su instancia y habilita una dirección IPv6 principal, la primera dirección GUA de IPv6 asociada al ENI pasa a ser la dirección IPv6 principal.

9. (Opcional) Para crear una Elastic Fabric Adapter, elija Elastic Fabric Adapter, Habilitar.
10. (Opcional) En Configuración avanzada, en Tiempo de espera del seguimiento de la conexión inactiva, modifique los tiempos de espera de la conexión inactiva predeterminados. Para obtener más información sobre estas opciones, consulte Tiempo de espera de seguimiento de conexiones inactivas.

    - Tiempo de espera establecido de TCP: tiempo de espera (en segundos) para las conexiones TCP inactivas en un estado establecido. Valor mínimo: 60 segundos. Valor máximo: 432 000 segundos (5 días). Valor predeterminado: 432 000 segundos. Valor recomendado: menos de 432 000 segundos.
    - Tiempo de espera de UDP: tiempo de espera (en segundos) para los flujos de UDP inactivos que solo han registrado tráfico en una sola dirección o en una sola transacción de solicitud-respuesta. Valor mínimo: 30 segundos. Valor máximo: 60 segundos. Valor predeterminado: 30 segundos.
    - Tiempo de espera del flujo de UDP: tiempo de espera (en segundos) para los flujos de UDP inactivos clasificados como flujos que han recibido más de una transacción de solicitud-respuesta. Valor mínimo: 60 segundos. Valor máximo: 180 segundos (3 minutos). Valor predeterminado: 180 segundos.
11. En Grupos de seguridad, seleccione uno o varios grupos de seguridad.
12. (Opcional) Para cada etiqueta, elija Agregar nueva etiqueta y especifique una clave y un valor de etiqueta opcional.
13. Elija Crear interfaz de red.

Para crear un interfaz de red 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 Acceder a Amazon EC2.

- create-network-interface (AWS CLI)
- New-EC2NetworkInterface (AWS Tools for Windows PowerShell)

Ver detalles sobre una interfaz de red

Puede ver todas las interfaces de red en su cuenta.

Para describir una interfaz de red con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Network Interfaces.
3. Para ver la página de detalles de una interfaz de red, seleccione el ID de la interfaz de red. Alternativamente, para ver información sin salir de la página de interfaces de red, seleccione la casilla de verificación de la interfaz de red.

Para describir una interfaz de red 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 Acceder a Amazon EC2.

- describe-network-interfaces (AWS CLI)
- Get-EC2NetworkInterface (AWS Tools for Windows PowerShell)

Para describir un atributo de interfaz de red 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 Acceder a Amazon EC2.

- describe-network-interface-attribute (AWS CLI)
- Get-EC2NetworkInterfaceAttribute (AWS Tools for Windows PowerShell)

Asociar una interfaz de red a una instancia

Puede adjuntar una interfaz de red a cualquier instancia de la misma zona de disponibilidad que la interfaz de red, ya sea utilizando la página Instancias o Interfaces de red de la consola de Amazon EC2. Como alternativa, puede especificar interfaces de red existentes cuando lance instancias.

> **Important**
>
> Para las instancias de EC2 de una subred solo IPv6, si adjunta una interfaz de red secundaria a la instancia, el nombre de host DNS privado de la segunda interfaz de red se resolverá en la primera dirección IPv6 de la primera interfaz de red de la instancia. Para obtener más información acerca de los nombres de host DNS privados de las instancias de EC2, consulte Tipos de nombres de host de instancias de Amazon EC2.

Si se libera la dirección IPv4 pública de la instancia, no recibe una nueva si tiene conectada más de una interfaz de red. Para obtener más información acerca del comportamiento de las direcciones IPv4 públicas, consulte Direcciones IPv4 públicas.

Instances page

Para asociar una interfaz de red a una instancia mediante la página Instancias.

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancias).
3. Seleccione la casilla de verificación de la instancia.
4. Elija Acciones, Redes, Asociar interfaz de red.
5. Elija una VPC. Si va a asociar una interfaz de red secundaria a la instancia, la interfaz de red puede residir en la misma VPC que la instancia o en una VPC diferente que posea (siempre que la interfaz de red esté en una subred que se encuentre en la misma zona de disponibilidad que la instancia). Esto le permite crear instancias con varios hosts en las VPC con diferentes configuraciones de red y seguridad.
6. Seleccione una interfaz de red. Si la instancia admite varias tarjetas de red, puede elegir una tarjeta de red.
7. Elija Adjuntar.

Network Interfaces page

Para asociar una interfaz de red a una instancia mediante la página Interfaces de red

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Network Interfaces.
3. Seleccione la casilla de verificación de la interfaz de red.
4. Elija Acciones, Asociar.
5. Elija una instancia. Si la instancia admite varias tarjetas de red, puede elegir una tarjeta de red.
6. Elija Attach (Adjuntar).

Para conectar una interfaz de red a una instancia 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 Acceder a Amazon EC2.

> **Note**
>
> Puede conectar una interfaz de red que esté en otra VPC (pero en la misma zona de disponibilidad) a una instancia mediante el comando AWS CLIattach-network-interface. No puede hacerlo mediante la AWS Management Console.

- attach-network-interface (AWS CLI)
- Add-EC2NetworkInterface (AWS Tools for Windows PowerShell)

Desasociar una interfaz de red de una instancia

Puede desconectar una interfaz de red secundaria asociada a una instancia de EC2 en cualquier momento utilizando las páginas Instancias o Interfaces de red de la consola de Amazon EC2.

Si intenta desconectar una interfaz de red adjunta a un recurso de otro servicio, como un equilibrador de carga de Elastic Load Balancing, una función de Lambda, un WorkSpace o una puerta de enlace de NAT, aparecerá un error que indicará que no tiene permiso para acceder al recurso. Para averiguar qué servicio creó el recurso adjunto a una interfaz de red, verifique la descripción de la interfaz de red. Si elimina el recurso, se elimina su interfaz de red.

Instances page

Para desconectar una interfaz de red de una instancia en la página Instances

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancias).
3. Seleccione la casilla de verificación de la instancia. Consulte la sección Interfaces de red de la pestaña Redes para comprobar que la interfaz de red está asociada a una instancia como interfaz de red secundaria.
4. Elija Acciones, Redes, Desconectar interfaz de red.
5. Seleccione la interfaz de red y elija Desconectar.

Network Interfaces page

Para desconectar una interfaz de red de una instancia en la página Network Interfaces

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Network Interfaces.
3. Seleccione la casilla de verificación de la interfaz de red. Consulte la sección Detalles de la instancia de la pestaña Detalles para comprobar que la interfaz de red está asociada a una instancia como interfaz de red secundaria.
4. Elija Acciones, Desasociar.
5. Cuando se le indique que confirme, elija Desasociar.
6. Si la interfaz de red no se desconecta de la instancia, elija Forzar desconexión, Habilitar y vuelva a intentarlo. Recomendamos que forzar desconexión se emplee solo como último recurso. Forzar una desconexión puede impedir la conexión con una interfaz de red diferente en el mismo índice hasta que reinicie la instancia. También puede impedir que los metadatos de la instancia reflejen que la interfaz de red se desconectó hasta que reinicie la instancia.

Para desconectar una interfaz de red 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 Acceder a Amazon EC2.

- detach-network-interface (AWS CLI)
- Dismount-EC2NetworkInterface (AWS Tools for Windows PowerShell)

Administrar direcciones IP

Puede administrar las siguientes direcciones IP de las interfaces de red:

- Direcciones IP elásticas (una por cada dirección IPv4 privada)
- Direcciones IPv4
- Direcciones IPv6
- Dirección IPv6 principal

Para administrar las direcciones IP elásticas de una interfaz de red mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Network Interfaces.
3. Seleccione la casilla de verificación de la interfaz de red.
4. Para asociar una dirección IP elástica, haga lo siguiente:
    a. Elija Acciones, Asociar dirección.
    b. En Dirección IP elástica, seleccione la dirección IP elástica.
    c. En Dirección IP privada, seleccione la dirección IPv4 privada que desea asociar a la dirección IP elástica.
    d. (Opcional) Elija Permitir que se vuelva a asociar la dirección IP elástica si la interfaz de red está asociada actualmente a otra instancia o interfaz de red.
    e. Elija Associate.
5. Para desasociar una dirección IP elástica, haga lo siguiente:
    a. Elija Acciones, Desasociar dirección.
    b. En Dirección IP pública, seleccione la dirección IP elástica.
    c. Elija Disassociate (Desasociar).

Para administrar las direcciones IPv4 e IPv6 de una interfaz de red a través de la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Network Interfaces.
3. Seleccione la interfaz de red.
4. Elija Acciones, Administrar direcciones IP.
5. Amplíe la interfaz de red.
6. En Direcciones IPV4, modifique las direcciones IP tal y como sea necesario. Para asignar una dirección IPv4, elija Asignar nueva dirección IP y especifique una dirección IPv4 del rango de la subred o deje que AWS elija una por usted. Para anular la asignación de una dirección IPv4, elija Anular asignación junto a la dirección.
7. Para asignar o desasignar una dirección IPv4 pública a una interfaz de red, seleccione Asignar de manera automática una IP pública. Esta opción puede habilitarse o deshabilitarse en cualquier interfaz de red, pero solo se aplicará a la interfaz de red principal (eth0).

8. En Direcciones IPv6, modifique las direcciones IP según sea necesario. Para asignar una dirección IPv6, elija Asignar nueva dirección IP y especifique una dirección IPv6 del rango de la subred o deje que AWS elija una por usted. Para anular la asignación de una dirección IPv6, elija Anular asignación junto a la dirección.
9. (Opcional) Si modifica una interfaz de red en una subred de doble pila o solo para IPv6, tiene la opción de asignar la IP IPv6 principal. La asignación de una dirección IPv6 principal le permite evitar interrumpir el tráfico a las instancias o ENI. Escoja Habilitar si la instancia a la que se adjuntará este ENI depende de que su dirección IPv6 no cambie. AWS asignará automáticamente una dirección IPv6 asociada al ENI adjunto a la instancia como la dirección IPv6 principal. Una vez que habilite una dirección GUA de IPv6 para que sea la IPv6 principal, no podrá deshabilitarla. Al habilitar una dirección GUA de IPv6 para que sea una de IPv6 principal, la primera dirección GUA de IPv6 pasará a ser la dirección IPv6 principal hasta que se termine la instancia o se separe la interfaz de red. Si tiene varias direcciones IPv6 asociadas a un ENI adjunto a su instancia y habilita una dirección IPv6 principal, la primera dirección GUA de IPv6 asociada al ENI pasa a ser la dirección IPv6 principal.
10. Seleccione Guardar.

Para administrar las direcciones IP de una interfaz de red utilizando AWS CLI

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

- assign-ipv6-addresses
- associate-address
- disassociate-address
- unassign-ipv6-addresses

Para administrar las direcciones IP de una interfaz de red utilizando Tools for Windows PowerShell

Puede utilizar uno de los siguientes comandos.

- Register-EC2Address
- Register-EC2Ipv6AddressList
- Unregister-EC2Address
- Unregister-EC2Ipv6AddressList

Modificar atributos de interfaz de red

Puede cambiar los siguientes atributos de la interfaz de red:

- Descripción
- Grupos de seguridad
- Eliminar al terminar
- Comprobación de origen/destino

Para cambiar la descripción de una interfaz de red a través de la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Network Interfaces.
3. Seleccione la casilla de verificación de la interfaz de red.
4. Elija Acciones, Cambiar descripción.
5. En Descripción, escriba una descripción para la interfaz de red.
6. Seleccione Save.

Para cambiar los grupos de seguridad de una interfaz de red a través de la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Network Interfaces.
3. Seleccione la casilla de verificación de la interfaz de red.
4. Elija Acciones, Cambiar grupos de seguridad.
5. En Grupos de seguridad asociados, seleccione los grupos de seguridad que desea utilizar y elija Guardar.

   El grupo de seguridad y la interfaz de red deben crearse para la misma VPC. Si desea cambiar el grupo de seguridad de unas interfaces que son propiedad de otros servicios (por ejemplo, Elastic Load Balancing), hágalo a través del servicio correspondiente.

Para cambiar el comportamiento de terminación de una interfaz de red a través de la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Network Interfaces.
3. Seleccione la casilla de verificación de la interfaz de red.
4. Elija Acciones, Cambiar el comportamiento de terminación.
5. Seleccione o borre Eliminar al terminar, Habilitar según sea necesario y, a continuación, elija Guardar.

Para cambiar la comprobación de origen/destino de una interfaz de red con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Network Interfaces.
3. Seleccione la casilla de verificación de la interfaz de red.
4. Elija Acciones, Cambiar comprobación de origen/destino.
5. Seleccione o borre Comprobación de origen/destino, Habilitar según sea necesario y, a continuación, elija Guardar.

Para cambiar los tiempos de espera de seguimiento de conexiones inactivas:

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Network Interfaces.
3. Seleccione la casilla de verificación de la interfaz de red.
4. Seleccione Acciones y Modificar tiempo de espera de conexión.
5. Modifique los tiempos de espera de seguimiento de conexiones inactivas. Para obtener más información sobre estas opciones, consulte Tiempo de espera de seguimiento de conexiones inactivas.

   - Tiempo de espera establecido de TCP: tiempo de espera (en segundos) para las conexiones TCP inactivas en un estado establecido. Valor mínimo: 60 segundos. Valor máximo: 432 000 segundos (5 días). Valor predeterminado: 432 000 segundos. Valor recomendado: menos de 432 000 segundos.

- Tiempo de espera de UDP: tiempo de espera (en segundos) para los flujos de UDP inactivos que solo han registrado tráfico en una sola dirección o en una sola transacción de solicitud-respuesta. Valor mínimo: 30 segundos. Valor máximo: 60 segundos. Valor predeterminado: 30 segundos.
- Tiempo de espera del flujo de UDP: tiempo de espera (en segundos) para los flujos de UDP inactivos clasificados como flujos que han recibido más de una transacción de solicitud-respuesta. Valor mínimo: 60 segundos. Valor máximo: 180 segundos (3 minutos). Valor predeterminado: 180 segundos.

6. Seleccione Guardar.

Para modificar los atributos de la interfaz de red a través de la línea de comandos

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

- modify-network-interface-attribute (AWS CLI)
- Edit-EC2NetworkInterfaceAttribute (AWS Tools for Windows PowerShell)

Agregar o editar etiquetas

Las etiquetas son metadatos que puede agregar a una interfaz de red. Las etiquetas son privadas y solo visibles en su cuenta. Cada etiqueta consta de una clave y un valor opcional. Para obtener más información acerca de las etiquetas, consulte Etiquetar los recursos de Amazon EC2.

Para agregar o modificar las etiquetas de una interfaz de red con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Network Interfaces.
3. Seleccione la casilla de verificación de la interfaz de red.
4. En la pestaña Etiquetas, elija Administrar etiquetas.
5. Para cada etiqueta que se cree, elija Agregar nueva etiqueta e introduzca una clave y un valor opcional. Cuando haya terminado, elija Guardar.

Para agregar o modificar las etiquetas de una interfaz de red 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 Acceder a Amazon EC2.

- create-tags (AWS CLI)
- New-EC2Tag (AWS Tools for Windows PowerShell)

Eliminar una interfaz de red

Al eliminar la interfaz de red se liberan todos los atributos que tiene asociados, así como todas las direcciones IP privadas o elásticas para que las utilice otra instancia.

No puede eliminar una interfaz de red que esté en uso. En primer lugar, debe desconectar la interfaz de red.

Para eliminar una interfaz de red con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Network Interfaces.
3. Seleccione la casilla de verificación para la interfaz de red y, a continuación, elija Acciones, Borrar.
4. Cuando se le pida confirmación, seleccione Delete (Eliminar).

Para eliminar una interfaz de red 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 Acceder a Amazon EC2.

- delete-network-interface (AWS CLI)
- Remove-EC2NetworkInterface (AWS Tools for Windows PowerShell)

Prácticas recomendadas para configurar interfaces de red

- Puede conectar una interfaz de red a una instancia cuando está ejecutándose (ajuste en caliente), cuando se detiene (ajuste templado) o cuando se está iniciando (ajuste en frío).

- Puede desconectar las interfaces de red secundarias cuando la instancia esté detenida o en ejecución. Sin embargo, no puede desconectar la interfaz de red principal.
- Puede mover una interfaz de red secundaria de una instancia a otra, si las instancias están en la misma zona de disponibilidad y VPC pero en subredes diferentes.
- Cuando se inicia una instancia utilizando la CLI, la API o un SDK, puede especificar la interfaz de red principal e interfaces de red adicionales.
- Cuando se inicia una instancia de Amazon Linux o Windows Server con varias interfaces de red, se configuran automáticamente las interfaces, las direcciones IPv4 privadas y las tablas de enrutamiento en el sistema operativo de la instancia.
- Una conexión en caliente o templada de una interfaz de red adicional podría requerir que active manualmente la segunda interfaz, configure la dirección IPv4 privada y modifique la tabla de enrutamiento en consecuencia. Las instancias que ejecutan Amazon Linux o Windows Server reconocen automáticamente la conexión en caliente o templada, y se autoconfiguran.
- No puede adjuntar otra interfaz de red a una instancia (por ejemplo, una configuración de NIC Teaming) para aumentar o duplicar el ancho de banda de la red desde o hacia la instancia con doble alojamiento.
- Si asocia dos o más interfaces de red de la misma subred a una instancia, pueden producirse problemas de red, como el direccionamiento asimétrico. Si es posible, en su lugar, use una dirección IPv4 privada secundaria en la interfaz de red principal.
- Instancias de Windows: si tiene que usar varias interfaces de red, debe configurarlas para que utilicen el direccionamiento estático.

Configure su interfaz de red mediante ec2-net-utils para Amazon Linux 2

> **Note**
>
> En el caso de AL2023, el paquete `amazon-ec2-net-utils` genera configuraciones específicas de la interfaz en el directorio `/run/systemd/network`. Para obtener más información, consulte Servicio de red en la Guía del usuario de Amazon Linux 2023 de .

Las AMI de Amazon Linux 2 pueden contener scripts adicionales que AWS instala, conocidos como ec2-net-utils. Estos scripts automatizan opcionalmente la configuración de las interfaces de red. Estos scripts solo están disponibles para Amazon Linux 2.

Utilice el siguiente comando para instalar el paquete en Amazon Linux 2 en caso de que aún no esté instalado, o actualícelo si lo está; hay actualizaciones adicionales disponibles:

```
$ yum install ec2-net-utils
```

Los componentes siguientes forman parte de ec2-net-utils:

Reglas udev (`/etc/udev/rules.d`)

Identifica las interfaces de red cuando se han conectado, desconectado o vuelto a conectar a una instancia en ejecución, y se asegura de que se ejecuta el script de conexión en caliente (`53-ec2-network-interfaces.rules`). Asigna la dirección MAC a un nombre de dispositivo (`75-persistent-net-generator.rules`, que genera `70-persistent-net.rules`).

script de conexión en caliente

Genera un archivo de configuración de interfaz adecuado para usarlo con DHCP (`/etc/sysconfig/network-scripts/ifcfg-ethN`). También genera un archivo de configuración de ruta (`/etc/sysconfig/network-scripts/route-ethN`).

script DHCP

Siempre que la interfaz de red recibe una nueva concesión DHCP, este script consulta los metadatos de la instancia en busca de direcciones IP elásticas. Para cada dirección IP elástica, agrega una regla a la base de datos de la política de direccionamiento que asegura que el tráfico saliente de dicha dirección utiliza la interfaz de red correcta. También agrega cada dirección IP privada a la interfaz de red como dirección secundaria.

ec2ifup ethN (`/usr/sbin/`)

Amplía la funcionalidad de ifup estándar. Después de que el script vuelve a escribir los archivos de configuración `ifcfg-ethN` y `route-ethN`, ejecuta ifup.

ec2ifdown ethN (`/usr/sbin/`)

Amplía la funcionalidad de ifdown estándar. Después de que este script elimina todas las reglas de la interfaz de red de la base de datos de la política de direccionamiento, ejecuta ifdown.

ec2ifscan (`/usr/sbin/`)

Comprueba las interfaces de red que no se han configurado y las configura.

Este script no está disponible en la versión inicial de ec2-net-utils.

Para enumerar los archivos de configuración generados por ec2-net-utils, use el comando siguiente:

```
$ ls -l /etc/sysconfig/network-scripts/*-eth?
```

Para desactivar la automatización, puede agregar `EC2SYNC=no` al archivo `ifcfg-eth`N correspondiente. Por ejemplo, use el comando siguiente para deshabilitar la automatización de la interfaz eth1:

```
$ sed -i -e 's/^EC2SYNC=yes/EC2SYNC=no/' /etc/sysconfig/network-scripts/ifcfg-eth1
```

Para deshabilitar la automatización completamente, puede quitar el paquete con el comando siguiente:

```
$ yum remove ec2-net-utils
```

Caso de uso de las interfaces de red

Conectar varias interfaces de red a una instancia es útil cuando quiere:

- Crear una red de administración.
- Usar dispositivos de seguridad y redes en la nube privada virtual (VPC).
- Crear instancias de doble alojamiento con cargas de trabajo/funciones en subredes diferentes.
- Crear una solución de bajo presupuesto y elevada disponibilidad.

Crear una red de administración

Este escenario describe cómo puede crear una red de administración con interfaces de red, teniendo en cuenta los siguientes criterios y opciones de configuración (a continuación se muestra la imagen).

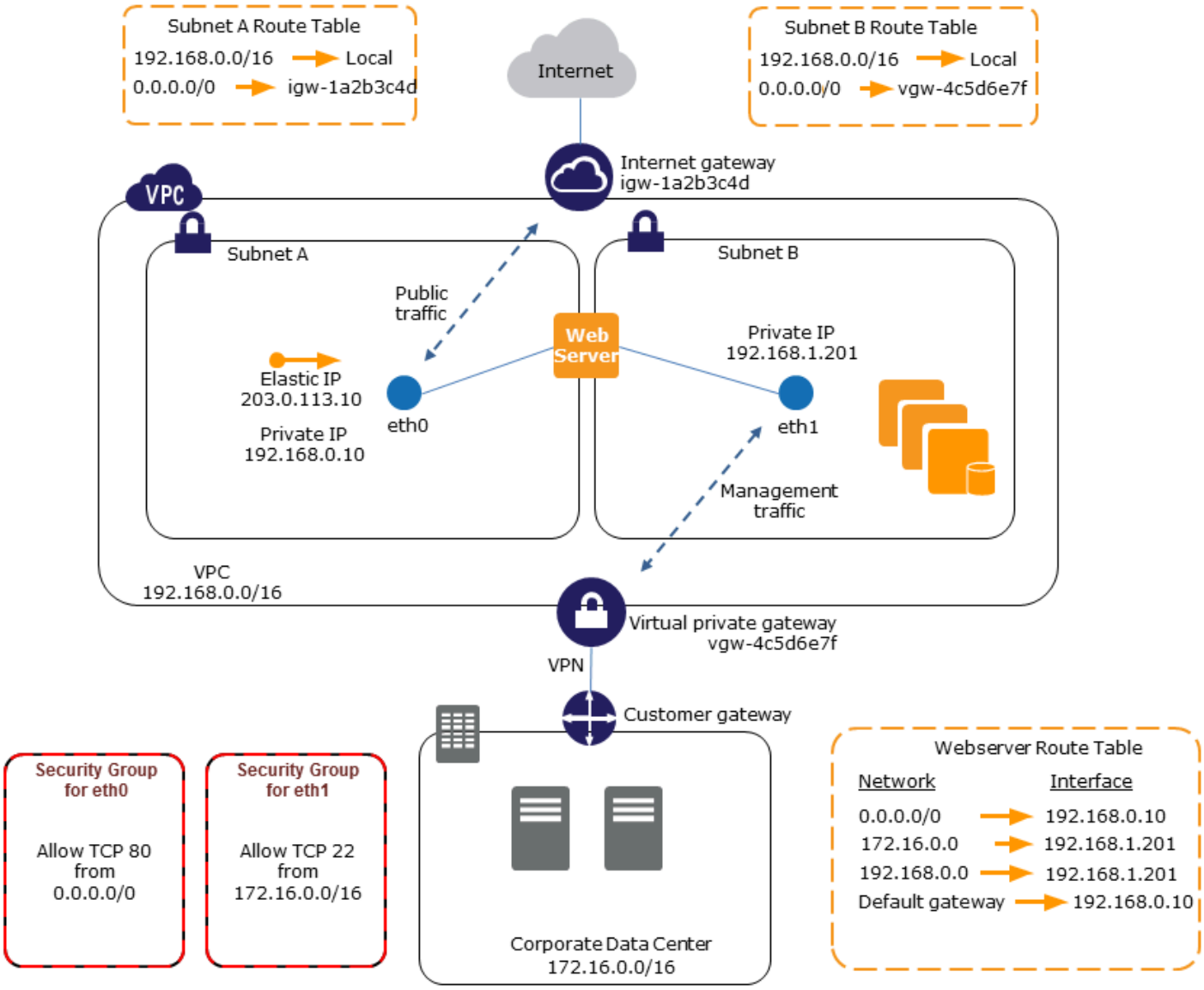
Criterios

- La interfaz de red principal de la instancia (eth0) gestiona el tráfico público.
- La interfaz de red secundaria de la instancia (eth1) gestiona el tráfico de administración del backend. Está conectada a una subred independiente que tiene controles de acceso más restrictivos y está ubicada en la misma zona de disponibilidad (AZ) que la interfaz de red principal.

Configuración

- La interfaz de red principal, que puede o no estar detrás de un equilibrador de carga, tiene un grupo de seguridad asociado que permite el acceso al servidor desde Internet. Por ejemplo, permite los puertos TCP 80 y 443 desde `0.0.0.0/0` o desde el equilibrador de carga.
- La interfaz de red secundaria tiene un grupo de seguridad asociado que solo permite el acceso a SSH, iniciado desde una de las siguientes ubicaciones:
  - Un rango permitido de direcciones IP, ya sea dentro de la VPC o desde Internet.
  - Una subred privada dentro de la misma AZ que la interfaz de red principal.
  - Una puerta de enlace privada virtual.

> **Note**
>
> Para asegurar la capacidad de conmutación por error, considere el uso de una IPv4 privada secundaria para el tráfico entrante en una interfaz de red. En caso de que se produzca un error en una instancia, puede mover la interfaz y/o la dirección IPv4 privada secundaria a una instancia en espera.



Uso de dispositivos de red y seguridad en la VPC

Algunos dispositivos de red y seguridad, como los balanceadores de carga, los servidores NAT (network address translation) y los servidores proxy prefieren estar configurados con varias interfaces de red. Puede crear y adjuntar interfaces de red secundarias a instancias que ejecuten estos tipos de aplicaciones y configurar las interfaces adicionales con sus propias direcciones IP privadas y públicas, grupos de seguridad y comprobaciones de origen/destino.

Creación de instancias de doble alojamiento con cargas de trabajo/roles en subredes diferentes

Puede ubicar una interfaz de red en cada servidor web que se conecte a una red de capa intermedia donde reside el servidor de aplicaciones. El servidor de aplicaciones también puede tener doble alojamiento en una red de backend (subred) donde reside el servidor de bases de datos. En lugar de enrutar los paquetes de red a través de las instancias de doble alojamiento, cada una de estas instancias recibe y procesa las solicitudes en el front end, inicia una conexión con el backend y envía las solicitudes a los servidores en la red backend.

Creación de instancias de doble host con cargas de trabajo o roles en VPC diferentes con la misma cuenta

Puede iniciar una instancia de EC2 en una VPC y adjuntar una ENI secundaria de otra VPC (pero en la misma zona de disponibilidad) a la instancia. Esto le permite crear instancias con varios hosts en las VPC con diferentes configuraciones de red y seguridad. No puede crear instancias con varios hosts en las VPC de cuentas de AWS diferentes.

Puede usar instancias de doble host en las VPC en los siguientes casos de uso:

- Superar las superposiciones de CIDR entre dos VPC que no se pueden emparejar entre sí: puede utilizar un CIDR secundario en una VPC y permitir que una instancia se comunique a través de dos rangos de IP que no se superpongan.
- Conectar varias VPC en una sola cuenta: habilite la comunicación entre recursos individuales que normalmente estarían separados por los límites de las VPC.

Crear una solución de bajo presupuesto y elevada disponibilidad

Si una de las instancias que da servicio a una función particular da error, su interfaz de red puede conectarse a una instancia de reemplazo o de espera activa preconfigurada para el mismo rol, con el fin de recuperar rápidamente el servicio. Por ejemplo, puede usar una interfaz de red como principal o secundaria en un servicio crítico, como una instancia de la base de datos o una instancia NAT. Si la instancia da error (o más probable, el código que se ejecuta en su nombre) puede conectar la interfaz de red a una instancia en espera activa. Dado que la interfaz mantiene las direcciones IP privadas, direcciones IP elásticas y direcciones MAC, el tráfico de red comienza a fluir hacia la instancia en espera tan pronto como conecte la interfaz de red a la instancia de sustitución. Los usuarios experimentan una breve pérdida de conexión entre el momento en que la instancia da error

y el momento en que la interfaz de red se adjunta a la instancia en espera, pero no es necesario efectuar ningún cambio en la tabla de enrutamiento ni en el servidor DNS.

Interfaces de red administradas por el solicitante

Una interfaz de red administrada por el solicitante es una interfaz de red creada por Servicio de AWS en su VPC en su nombre. La interfaz de red está asociada a un recurso de otro servicio, como una instancia de la base de datos de Amazon RDS, una puerta de enlace de NAT o un punto de conexión de VPC de interfaz de AWS PrivateLink.

Consideraciones

- Puede ver las interfaces de red administrada por el solicitante en su cuenta. Puede agregar o eliminar etiquetas, pero no puede cambiar otras propiedades de una interfaz de red administrada por el solicitante.
- No es posible desconectar una interfaz de red administrada por el solicitante.
- Si elimina el recurso asociado a la interfaz de red administrada por el solicitante, el Servicio de AWS desconectará la interfaz de red y la eliminará. Si el servicio desconectó una interfaz de red pero no la eliminó, puede eliminar la interfaz de red desconectada.

Para ver las interfaces de red administradas por el solicitante mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Red y seguridad y, a continuación, Interfaces de red.
3. Seleccione el ID de la interfaz de red para abrir su página de detalles.
4. Los siguientes son los campos clave que puede utilizar para determinar el propósito de la interfaz de red:

   - Descripción: descripción proporcionada por el servicio de AWS que creó la interfaz. Por ejemplo, “Interfaz de punto de conexión de VPC vpce 089f2123488812123”.
   - Administrado por el solicitante: indica si la interfaz de red está administrada por AWS.
   - ID del solicitante: alias o ID de la cuenta de AWS de la entidad principal o el servicio que creó la interfaz de red. Si usted creó la interfaz de red, este es el ID de su Cuenta de AWS. De lo contrario, otra entidad principal o servicio lo creó.

Para ver las interfaces de red administradas por el solicitante mediante la AWS CLI

Utilice el comando describe-network-interfaces de la siguiente manera.

```
aws ec2 describe-network-interfaces --filters Name=requester-managed,Values=true
```

A continuación, se presenta el resultado de ejemplo que muestra los campos clave que puede utilizar para determinar el propósito de la interfaz de red: `Description` e `InterfaceType`.

```
{
     ...
    "Description": "VPC Endpoint Interface vpce-089f2123488812123",
    ...
    "InterfaceType": "vpc_endpoint",
    ...
    "NetworkInterfaceId": "eni-0d11e3ccd2c0e6c57",
    ...
    "RequesterId": "727180483921",
    "RequesterManaged": true,
    ...
}
```

Para ver las interfaces de red administradas por el solicitante mediante las herramientas para Windows PowerShell

Utilice cmdlet Get-EC2NetworkInterface de la siguiente manera.

```
Get-EC2NetworkInterface -Filter @{ Name="requester-managed"; Values="true" }
```

A continuación, se presenta el resultado de ejemplo que muestra los campos clave que puede utilizar para determinar el propósito de la interfaz de red: `Description` e `InterfaceType`.

```
Description        : VPC Endpoint Interface vpce-089f2123488812123
...
InterfaceType      : vpc_endpoint
...
NetworkInterfaceId : eni-0d11e3ccd2c0e6c57
...
RequesterId        : 727180483921
RequesterManaged   : True
...
```

Asigne prefijos a las interfaces de red de Amazon EC2

Puede asignar un intervalo CIDR IPv4 o IPv6 privado, ya sea de forma automática o manual, a las interfaces de red. Al asignar prefijos, puede escalar y simplificar la administración de aplicaciones, incluidas las aplicaciones de red y contenedores que requieren varias direcciones IP en una instancia. Para obtener más información acerca de las direcciones IPv4 e IPv6, consulte Direccionamiento IP de instancias Amazon EC2.

Están disponibles las siguientes opciones de asignación:

- Asignación automática: AWS elige el prefijo del bloque de CIDR de la IPv4 o IPv6 de su subred de VPC y lo asigna a la interfaz de red.
- Asignación manual: tiene que especificar el prefijo del bloque de CIDR de la IPv4 o IPv6 de su subred de VPC. AWS comprueba que el prefijo no se haya asignado a otros recursos antes de asignarlo a la interfaz de red.

La asignación de prefijos incluye los siguientes beneficios:

- Mayor número de direcciones IP en una interfaz de red: cuando se utiliza un prefijo, se asigna un bloque de direcciones IP en lugar de direcciones IP individuales. Esto aumenta el número de direcciones IP en una interfaz de red.
- Administración simplificada de VPC para contenedores: en las aplicaciones de contenedores, cada contenedor requiere una dirección IP única. La asignación de prefijos a la instancia simplifica la gestión de las VPC, ya que puede iniciar y finalizar contenedores sin tener que llamar a las API de Amazon EC2 para asignaciones de IP individuales.

Contenido

Conceptos básicos para asignar prefijos

- Puede asignar un prefijo a interfaces de red nuevas o existentes.
- Para utilizar prefijos, primero asigne un prefijo a su interfaz de red; luego, adjunte la interfaz de red a su instancia y, a continuación, configure el sistema operativo.

- Cuando elige la opción para especificar un prefijo, el prefijo debe cumplir los siguientes requisitos:
  - El prefijo IPv4 que puede especificar es `/28`.
  - El prefijo IPv6 que puede especificar es `/80`.
  - El prefijo se encuentra en el CIDR de la subred de la interfaz de red y no se superpone con otros prefijos o direcciones IP asignados a recursos existentes en la subred.
- Puede asignar un prefijo a la interfaz de red principal o secundaria.
- Puede asignar una dirección IP elástica a una interfaz de red que tenga un prefijo asignado.
- También puede asignar una dirección IP elástica a la parte de la dirección IP del prefijo asignado.
- Resolvemos el nombre de host DNS privado de una instancia en la dirección IPv4 privada.
- Se asigna cada dirección IPv4 privada a una interfaz de red, incluidas las de prefijos, con los siguientes formatos:
  - Región de `us-east-1`

    ```
    ip-private-ipv4-address.ec2.internal
    ```

  - Las demás regiones

    ```
    ip-private-ipv4-address.region.compute.internal
    ```

Consideraciones y límites para los prefijos

Tenga en cuenta lo siguiente cuando utilice prefijos:

- Las interfaces de red con prefijos son compatibles con las instancias integradas en el AWS Nitro System.
- Los prefijos de las interfaces de red están limitados a direcciones IPv6 y direcciones IPv4 privadas.
- El número máximo de direcciones IP que puede asignar a una interfaz de red depende del tipo de instancia. Cada prefijo que asigna a una interfaz de red cuenta como una dirección IP. Por ejemplo, una instancia `c5.large` tiene un límite de `10` direcciones IPv4 por interfaz de red. Cada interfaz de red de esta instancia tiene una dirección IPv4 principal. Si una interfaz de red no tiene direcciones IPv4 secundarias, puede asignar hasta 9 prefijos a la interfaz de red. Por cada dirección IPv4 adicional que asigne a una interfaz de red, puede asignar un prefijo menos a la interfaz de red. Para obtener más información, consulte Direcciones IP por interfaz de red por tipo de instancia.
- Los prefijos se incluyen en las comprobaciones de origen/destino.

Trabajar con prefijos

Puede utilizar prefijos en las interfaces de red de la siguiente manera.

Tareas

- Asignar prefijos durante la creación de la interfaz de red
- Asignar prefijos a las interfaces de red existentes
- Configurar el sistema operativo para las interfaces de red con prefijos
- Ver los prefijos asignados a las interfaces de red
- Eliminar prefijos de las interfaces de red

Asignar prefijos durante la creación de la interfaz de red

Si utiliza la opción de asignación automática, puede reservar un bloque de direcciones IP en la subred. AWS elige los prefijos desde este bloque. Para obtener más información, consulte Reservas de la subred de CIDR en la Guía del usuario de Amazon VPC.

Una vez que cree la interfaz de red, utilice el comando attach-network-interface de la AWS CLI para adjuntar la interfaz de red a la instancia. Debe configurar el sistema operativo para que trabaje con interfaces de red con prefijos. Para obtener más información, consulte Configurar el sistema operativo para las interfaces de red con prefijos.

Tareas

- Asignar prefijos automáticos durante la creación de la interfaz de red
- Asignar prefijos específicos durante la creación de la interfaz de red

Asignar prefijos automáticos durante la creación de la interfaz de red

Puede asignar prefijos automáticos durante la creación de la interfaz de red mediante uno de los siguientes métodos.

Console

Para asignar prefijos automáticos durante la creación de la interfaz de red

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Interfaces de red y, a continuación, Crear interfaz de red.

3. Especifique una descripción para la interfaz de red, seleccione la subred en la que desea crear la interfaz de red y configure las direcciones IPv4 e IPv6 privadas.
4. Expanda Configuración avanzada y realice una de las siguientes opciones:

   a. Para asignar de forma automática un prefijo IPv4, en Delegación de prefijos IPv4, elija Asignar de forma automática. Luego, en Número de prefijos IPv4, especifique el número de prefijos que desea asignar.

   b. Para asignar de forma automática un prefijo IPv6, en Delegación de prefijos IPv6, elija Asignar de forma automática. Luego, en Número de prefijos IPv6, especifique el número de prefijos que desea asignar.

   > **Note**
   >
   > Delegación de prefijos IPv6 solo aparece si la subred seleccionada se encuentra habilitada para IPv6.

5. Seleccione los grupos de seguridad que deben asociarse a la interfaz de red y, si es necesario, asigne etiquetas de recursos.
6. Elija Crear interfaz de red.

AWS CLI

Para asignar prefijos IPv4 automáticos durante la creación de la interfaz de red

Utilice el comando create-network-interface y establezca `--ipv4-prefix-count` en el número de prefijos que desea que AWS asigne. En el siguiente ejemplo, AWS asigna el prefijo 1.

```
$ C:\> aws ec2 create-network-interface \
--subnet-id subnet-047cfed18eEXAMPLE \
--description "IPv4 automatic example" \
--ipv4-prefix-count 1
```

Ejemplo de resultado

```
{
    "NetworkInterface": {
        "AvailabilityZone": "us-west-2a",
        "Description": "IPv4 automatic example",
        "Groups": [
```

```
            {
                "GroupName": "default",
                "GroupId": "sg-044c2de2c4EXAMPLE"
            }
        ],
        "InterfaceType": "interface",
        "Ipv6Addresses": [],
        "MacAddress": "02:98:65:dd:18:47",
        "NetworkInterfaceId": "eni-02b80b4668EXAMPLE",
        "OwnerId": "123456789012",
        "PrivateIpAddress": "10.0.0.62",
        "PrivateIpAddresses": [
            {
                "Primary": true,
                "PrivateIpAddress": "10.0.0.62"
            }
        ],
        "Ipv4Prefixes": [
            {
                "Ipv4Prefix": "10.0.0.208/28"
            }
        ],
        "RequesterId": "AIDAIV5AJI5LXF5XXDPCO",
        "RequesterManaged": false,
        "SourceDestCheck": true,
        "Status": "pending",
        "SubnetId": "subnet-047cfed18eEXAMPLE",
        "TagSet": [],
        "VpcId": "vpc-0e12f52b21EXAMPLE"
    }
}
```

Para asignar prefijos IPv6 automáticos durante la creación de la interfaz de red

Utilice el comando create-network-interface y establezca `--ipv6-prefix-count` en el número de prefijos que desea que AWS asigne. En el siguiente ejemplo, AWS asigna el prefijo 1.

```
$ C:\> aws ec2 create-network-interface \
--subnet-id subnet-047cfed18eEXAMPLE \
--description "IPv6 automatic example" \
--ipv6-prefix-count 1
```

Ejemplo de resultado

```
{
    "NetworkInterface": {
        "AvailabilityZone": "us-west-2a",
        "Description": "IPv6 automatic example",
        "Groups": [
            {
                "GroupName": "default",
                "GroupId": "sg-044c2de2c4EXAMPLE"
            }
        ],
        "InterfaceType": "interface",
        "Ipv6Addresses": [],
        "MacAddress": "02:bb:e4:31:fe:09",
        "NetworkInterfaceId": "eni-006edbcfa4EXAMPLE",
        "OwnerId": "123456789012",
        "PrivateIpAddress": "10.0.0.73",
        "PrivateIpAddresses": [
            {
                "Primary": true,
                "PrivateIpAddress": "10.0.0.73"
            }
        ],
        "Ipv6Prefixes": [
            {
                "Ipv6Prefix": "2600:1f13:fc2:a700:1768::/80"
            }
        ],
        "RequesterId": "AIDAIV5AJI5LXF5XXDPCO",
        "RequesterManaged": false,
        "SourceDestCheck": true,
        "Status": "pending",
        "SubnetId": "subnet-047cfed18eEXAMPLE",
        "TagSet": [],
        "VpcId": "vpc-0e12f52b21EXAMPLE"
    }
}
```


Asignar prefijos específicos durante la creación de la interfaz de red

Puede asignar prefijos específicos durante la creación de la interfaz de red mediante uno de los siguientes métodos.

Console

Para asignar prefijos específicos durante la creación de la interfaz de red

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Interfaces de red y, a continuación, Crear interfaz de red.
3. Especifique una descripción para la interfaz de red, seleccione la subred en la que desea crear la interfaz de red y configure las direcciones IPv4 e IPv6 privadas.
4. Expanda Advanced settings (Configuración avanzada) y realice una de las siguientes opciones:

   a. Para asignar un prefijo IPv4 específico, en Delegación de prefijos IPv4, elija Personalizado. A continuación, elija Agregar prefijo nuevo e ingrese el prefijo que desea utilizar.

   b. Para asignar un prefijo IPv6 específico, en Delegación de prefijos IPv6, elija Personalizado. A continuación, elija Add new prefix (Agregar prefijo nuevo) e ingrese el prefijo que desea utilizar.

   > **Note**
   >
   > IPv6 prefix delegation (Delegación de prefijos IPv6) solo aparece si la subred seleccionada se encuentra habilitada para IPv6.

5. Seleccione los grupos de seguridad que deben asociarse a la interfaz de red y, si es necesario, asigne etiquetas de recursos.
6. Elija Crear interfaz de red.

AWS CLI

Para asignar prefijos IPv4 específicos durante la creación de la interfaz de red

Utilice el comando create-network-interface y establezca `--ipv4-prefixes` en los prefijos. AWS selecciona direcciones IP de este rango. En el ejemplo siguiente, el prefijo CIDR es `10.0.0.208/28`.

```
$ C:\> aws ec2 create-network-interface \
    --subnet-id subnet-047cfed18eEXAMPLE \
    --description "IPv4 manual example" \
```

```
    --ipv4-prefixes Ipv4Prefix=10.0.0.208/28
```

Ejemplo de resultado

```
{
        "NetworkInterface": {
            "AvailabilityZone": "us-west-2a",
            "Description": "IPv4 manual example",
            "Groups": [
                {
                    "GroupName": "default",
                    "GroupId": "sg-044c2de2c4EXAMPLE"
                }
            ],
            "InterfaceType": "interface",
            "Ipv6Addresses": [],
            "MacAddress": "02:98:65:dd:18:47",
            "NetworkInterfaceId": "eni-02b80b4668EXAMPLE",
            "OwnerId": "123456789012",
            "PrivateIpAddress": "10.0.0.62",
            "PrivateIpAddresses": [
                {
                    "Primary": true,
                    "PrivateIpAddress": "10.0.0.62"
                }
            ],
            "Ipv4Prefixes": [
                {
                    "Ipv4Prefix": "10.0.0.208/28"
                }
            ],
            "RequesterId": "AIDAIV5AJI5LXF5XXDPCO",
            "RequesterManaged": false,
            "SourceDestCheck": true,
            "Status": "pending",
            "SubnetId": "subnet-047cfed18eEXAMPLE",
            "TagSet": [],
            "VpcId": "vpc-0e12f52b21EXAMPLE"
        }
    }
```

Para asignar prefijos IPv6 específicos durante la creación de la interfaz de red

Utilice el comando create-network-interface y establezca `--ipv6-prefixes` en los prefijos. AWS selecciona direcciones IP de este rango. En el ejemplo siguiente, el prefijo CIDR es `2600:1f13:fc2:a700:1768::/80`.

```
$ C:\> aws ec2 create-network-interface \
    --subnet-id subnet-047cfed18eEXAMPLE \
    --description "IPv6 manual example" \
    --ipv6-prefixes Ipv6Prefix=2600:1f13:fc2:a700:1768::/80
```

Ejemplo de resultado

```
{
        "NetworkInterface": {
            "AvailabilityZone": "us-west-2a",
            "Description": "IPv6 automatic example",
            "Groups": [
                {
                    "GroupName": "default",
                    "GroupId": "sg-044c2de2c4EXAMPLE"
                }
            ],
            "InterfaceType": "interface",
            "Ipv6Addresses": [],
            "MacAddress": "02:bb:e4:31:fe:09",
            "NetworkInterfaceId": "eni-006edbcfa4EXAMPLE",
            "OwnerId": "123456789012",
            "PrivateIpAddress": "10.0.0.73",
            "PrivateIpAddresses": [
                {
                    "Primary": true,
                    "PrivateIpAddress": "10.0.0.73"
                }
            ],
            "Ipv6Prefixes": [
                {
                    "Ipv6Prefix": "2600:1f13:fc2:a700:1768::/80"
                }
            ],
            "RequesterId": "AIDAIV5AJI5LXF5XXDPCO",
            "RequesterManaged": false,
            "SourceDestCheck": true,
            "Status": "pending",
            "SubnetId": "subnet-047cfed18eEXAMPLE",
```

```
            "TagSet": [],
            "VpcId": "vpc-0e12f52b21EXAMPLE"
        }
    }
```

Asignar prefijos a las interfaces de red existentes

Una vez que haya asignado los prefijos, utilice el comando attach-network-interface de la AWS CLI para adjuntar la interfaz de red a su instancia. Debe configurar el sistema operativo para que trabaje con interfaces de red con prefijos. Para obtener más información, consulte Configurar el sistema operativo para las interfaces de red con prefijos.

Tareas

- Asignar prefijos automáticos a una interfaz de red existente
- Asignar prefijos específicos a una interfaz de red existente

Asignar prefijos automáticos a una interfaz de red existente

Puede asignar prefijos automáticos a una interfaz de red existente mediante uno de los siguientes métodos.

Console

Para asignar prefijos automáticos a una interfaz de red existente

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Network Interfaces.
3. Seleccione la interfaz de red a la que desea asignar los prefijos y elija Acciones, Administrar prefijos.
4. Para asignar de forma automática un prefijo IPv4, en IPv4 prefix delegation (Delegación de prefijos IPv4), elija Auto-assign (Asignar de forma automática). Luego, en Número de prefijos IPv4, especifique el número de prefijos que desea asignar.
5. Para asignar de forma automática un prefijo IPv6, en Delegación de prefijos IPv6, elija Asignar de forma automática. Luego, en Número de prefijos IPv6, especifique el número de prefijos que desea asignar.

> **Note**
>
> IPv6 prefix delegation (Delegación de prefijos IPv6) solo aparece si la subred seleccionada se encuentra habilitada para IPv6.

6. Elija Save (Guardar).

AWS CLI

Puede utilizar el comando assign-ipv6-addresses para asignar prefijos IPv6 y el comando assign-private-ip-addresses para asignar prefijos IPv4 a las interfaces de red existentes.

Para asignar prefijos IPv4 automáticos a una interfaz de red existente

Utilice el comando assign-private-ip-addresses y establezca `--ipv4-prefix-count` en el número de prefijos que desea que asigne AWS. En el siguiente ejemplo, AWS asigna el prefijo 1 IPv4.

```
$ C:\> aws ec2 assign-private-ip-addresses \
--network-interface-id eni-081fbb4095EXAMPLE \
--ipv4-prefix-count 1
```

Ejemplo de resultado

```
{
    "NetworkInterfaceId": "eni-081fbb4095EXAMPLE",
    "AssignedIpv4Prefixes": [
        {
            "Ipv4Prefix": "10.0.0.176/28"
        }
    ]
}
```

Para asignar prefijos IPv6 automáticos a una interfaz de red existente

Utilice el comando assign-ipv6-addresses y establezca `--ipv6-prefix-count` en el número de prefijos que desea que asigne AWS. En el siguiente ejemplo, AWS asigna el prefijo 1 IPv6.

```
$ C:\> aws ec2 assign-ipv6-addresses \
```

```
--network-interface-id eni-00d577338cEXAMPLE \
--ipv6-prefix-count 1
```

Ejemplo de resultado

```
{
    "AssignedIpv6Prefixes": [
        "2600:1f13:fc2:a700:18bb::/80"
    ],
    "NetworkInterfaceId": "eni-00d577338cEXAMPLE"
}
```

Asignar prefijos específicos a una interfaz de red existente

Puede asignar prefijos específicos a una interfaz de red existente mediante uno de los siguientes métodos.

Console

Para asignar prefijos específicos a una interfaz de red existente

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Network Interfaces.
3. Seleccione la interfaz de red a la que desea asignar los prefijos y elija Actions (Acciones), Manage prefixed (Administrar prefijos).
4. Para asignar un prefijo IPv4 específico, en IPv4 prefix delegation (Delegación de prefijos IPv4), elija Custom (Personalizado). A continuación, elija Agregar prefijo nuevo e ingrese el prefijo que desea utilizar.
5. Para asignar un prefijo IPv6 específico, en Delegación de prefijos IPv6, elija Personalizado. A continuación, elija Add new prefix (Agregar prefijo nuevo) e ingrese el prefijo que desea utilizar.

   > **Note**
   >
   > IPv6 prefix delegation (Delegación de prefijos IPv6) solo aparece si la subred seleccionada se encuentra habilitada para IPv6.

6. Seleccione Guardar.

AWS CLI

Asignar prefijos IPv4 específicos a una interfaz de red existente

Utilice el comando assign-private-ip-addresses y establezca `--ipv4-prefixes` en el prefijo. AWS selecciona direcciones IPv4 de este rango. En el ejemplo siguiente, el prefijo CIDR es `10.0.0.208/28`.

```
$ C:\> aws ec2 assign-private-ip-addresses \
--network-interface-id eni-081fbb4095EXAMPLE \
--ipv4-prefixes 10.0.0.208/28
```

Ejemplo de resultado

```
{
    "NetworkInterfaceId": "eni-081fbb4095EXAMPLE",
    "AssignedIpv4Prefixes": [
        {
            "Ipv4Prefix": "10.0.0.208/28"
        }
    ]
}
```

Asignar prefijos IPv6 específicos a una interfaz de red existente

Utilice el comando assign-ipv6-addresses y establezca `--ipv6-prefixes` en el prefijo. AWS selecciona direcciones IPv6 de este rango. En el ejemplo siguiente, el prefijo CIDR es `2600:1f13:fc2:a700:18bb::/80`.

```
$ C:\> aws ec2 assign-ipv6-addresses \
--network-interface-id eni-00d577338cEXAMPLE \
--ipv6-prefixes 2600:1f13:fc2:a700:18bb::/80
```

Ejemplo de resultado

```
{
    "NetworkInterfaceId": "eni-00d577338cEXAMPLE",
    "AssignedIpv6Prefixes": [
        {
            "Ipv6Prefix": "2600:1f13:fc2:a700:18bb::/80"
        }
    ]
```

```
}
```

Configurar el sistema operativo para las interfaces de red con prefijos

Las AMI de Amazon Linux pueden contener otros scripts que instala AWS, conocidos como `ec2-net-utils`. Estos scripts automatizan opcionalmente la configuración de las interfaces de red. Solo son están disponibles para Amazon Linux.

Si no está utilizando Amazon Linux, puede utilizar una interfaz de red de contenedores (CNI) para el complemento de Kubernetes o `dockerd` si usa Docker para administrar sus contenedores.

Ver los prefijos asignados a las interfaces de red

Puede ver los prefijos asignados a la interfaz de red mediante uno de los siguientes métodos.

Console

Para ver prefijos automáticos asignados a una interfaz de red existente

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Network Interfaces.
3. Seleccione la interfaz de red para la que desea ver los prefijos y elija la pestaña Details (Detalles).
4. En el campo IPv4 Prefix Delegation (Delegación de Prefijo IPv4), se enumeran los prefijos IPv4 asignados y, en el campo IPv6 Prefix Delegation (Delegación de Prefijo IPv6), se enumeran los prefijos IPv6 asignados.

AWS CLI

Puede utilizar el comando describe-network-interfaces de AWS CLIpara ver los prefijos asignados a las interfaces de red.

```
$ C:\> aws ec2 describe-network-interfaces
```

Ejemplo de resultado

```
{
    "NetworkInterfaces": [
        {
```

```
            "AvailabilityZone": "us-west-2a",
            "Description": "IPv4 automatic example",
            "Groups": [
                {
                    "GroupName": "default",
                    "GroupId": "sg-044c2de2c4EXAMPLE"
                }
            ],
            "InterfaceType": "interface",
            "Ipv6Addresses": [],
            "MacAddress": "02:98:65:dd:18:47",
            "NetworkInterfaceId": "eni-02b80b4668EXAMPLE",
            "OwnerId": "123456789012",
            "PrivateIpAddress": "10.0.0.62",
            "PrivateIpAddresses": [
                {
                    "Primary": true,
                    "PrivateIpAddress": "10.0.0.62"
                }
            ],
            "Ipv4Prefixes": [
                {
                    "Ipv4Prefix": "10.0.0.208/28"
                }
            ],
            "Ipv6Prefixes": [],
            "RequesterId": "AIDAIV5AJI5LXF5XXDPCO",
            "RequesterManaged": false,
            "SourceDestCheck": true,
            "Status": "available",
            "SubnetId": "subnet-05eef9fb78EXAMPLE",
            "TagSet": [],
            "VpcId": "vpc-0e12f52b2146bf252"
        },
        {
            "AvailabilityZone": "us-west-2a",
            "Description": "IPv6 automatic example",
            "Groups": [
                {
                    "GroupName": "default",
                    "GroupId": "sg-044c2de2c411c91b5"
                }
            ],
            "InterfaceType": "interface",
```

```
            "Ipv6Addresses": [],
            "MacAddress": "02:bb:e4:31:fe:09",
            "NetworkInterfaceId": "eni-006edbcfa4EXAMPLE",
            "OwnerId": "123456789012",
            "PrivateIpAddress": "10.0.0.73",
            "PrivateIpAddresses": [
                {
                    "Primary": true,
                    "PrivateIpAddress": "10.0.0.73"
                }
            ],
            "Ipv4Prefixes": [],
            "Ipv6Prefixes": [
                {
                    "Ipv6Prefix": "2600:1f13:fc2:a700:1768::/80"
                }
            ],
            "RequesterId": "AIDAIV5AJI5LXF5XXDPCO",
            "RequesterManaged": false,
            "SourceDestCheck": true,
            "Status": "available",
            "SubnetId": "subnet-05eef9fb78EXAMPLE",
            "TagSet": [],
            "VpcId": "vpc-0e12f52b21EXAMPLE"
        }
    ]
}
```


Eliminar prefijos de las interfaces de red

Puede eliminar los prefijos de la interfaz de red mediante uno de los siguientes métodos.

Console

Para quitar prefijos de una interfaz de red

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Network Interfaces.
3. Seleccione la interfaz de red desde la que desea eliminar los prefijos y elija Actions (Acciones), Manage prefixed (Administrar prefijos).
4. Realice una de las siguientes acciones siguientes:

- Para quitar todos los prefijos asignados, en IPv4 prefix delegation (Delegación de prefijos IPv4) y IPv6 prefix delegation (Delegación de prefijos IPv6), elija Do not assign (No asignar).
- Para eliminar prefijos específicos asignados, en Delegación de prefijos IPv4 o Delegación de prefijos IPv6, elija Personalizar y luego Anular asignación junto a los prefijos que desee eliminar.

> **Note**
>
> IPv6 prefix delegation (Delegación de prefijos IPv6) solo aparece si la subred seleccionada se encuentra habilitada para IPv6.

5. Seleccione Guardar.

AWS CLI

Puede utilizar el comando unassign-ipv6-addresses para eliminar los prefijos IPv6 y el comando unassign-private-ip-addresses para quitar prefijos IPv4 de las interfaces de red existentes.

Para quitar prefijos IPv4 de una interfaz de red

Utilice el comando unassign-private-ip-addresses y establezca `--ipv4-prefix` en la dirección que desee quitar.

```
$ C:\> aws ec2 unassign-private-ip-addresses \
--network-interface-id eni-081fbb4095EXAMPLE \
--ipv4-prefixes 10.0.0.176/28
```

Para quitar prefijos IPv6 de una interfaz de red

Utilice el comando unassign-ipv6-addresses y establezca `--ipv6-prefix` en la dirección que desee quitar.

```
$ C:\> aws ec2 unassign-ipv6-addresses \
--network-interface-id eni-00d577338cEXAMPLE \
--ipv6-prefix 2600:1f13:fc2:a700:18bb::/80
```

Ancho de banda de red de instancias de Amazon EC2

Las especificaciones de ancho de banda de instancia se aplican al tráfico entrante y saliente de la instancia. Por ejemplo, si una instancia especifica hasta 10 Gbps de ancho de banda, eso significa que tiene hasta 10 Gbps de ancho de banda para el tráfico entrante y hasta 10 Gbps para el tráfico saliente. El ancho de banda de la red disponible para una instancia de EC2 depende de varios factores, como se indica a continuación.

Tráfico multiflujo

La banda ancha para el tráfico multiflujo agregado disponible para una instancia depende del destino del tráfico.

- El tráfico puede utilizar todo el ancho de banda de la red disponible para la instancia.
- A otras regiones, una puerta de enlace de Internet, Direct Connect o puertas de enlace locales (LGW): el tráfico puede utilizar hasta el 50 % del ancho de banda de la red disponible para una instancia de generación actual con un mínimo de 32 vCPUs. La banda ancha para una instancia de generación actual con menos de 32 vCPU se encuentra limitada a 5 Gbps.

Tráfico de flujo único

El ancho de banda de referencia para el tráfico de flujo único está limitado a 5 Gbps cuando las instancias no están en el mismo grupo con ubicación en clúster. Para reducir la latencia y aumentar el ancho de banda de flujo único, pruebe uno de los siguientes procedimientos:

- Utilice un grupo con ubicación en clúster para lograr un ancho de banda de hasta 10 Gbps para las instancias del mismo grupo de ubicación.
- Configure varias rutas entre dos puntos de conexión para lograr un mayor ancho de banda con Multipath TCP (MPTCP).
- Configure ENA Express para las instancias válidas de la misma subred para lograr hasta 25 Gbps entre esas instancias.

Ancho de banda de instancias disponible

La banda ancha de red disponible de una instancia depende del número de vCPU que tenga. Por ejemplo, una instancia `m5.8xlarge` tiene 32 vCPU y una banda ancha de red de 10 Gbps, y una instancia `m5.16xlarge` tiene 64 vCPU y una banda ancha de red de 20 Gbps. Sin embargo, es

posible que las instancias no alcancen esta banda ancha, por ejemplo, si superan los límites de red en el nivel de instancia, como paquete por segundo o número de conexiones rastreadas. La cantidad de banda ancha disponible que puede utilizar el tráfico depende del número de vCPU y del destino. Por ejemplo, una instancia `m5.16xlarge` tiene 64 vCPU, por lo que el tráfico a otra instancia de la región puede utilizar la banda ancha completa disponible (20 Gbps). Sin embargo, el tráfico a otra instancia en una región diferente solo puede utilizar el 50 % de la banda ancha disponible (10 Gbps).

Normalmente, las instancias con 16 vCPU o menos (tamaño `4xlarge` y más pequeños) están documentadas como “con hasta” una banda ancha especificada; por ejemplo, “hasta 10 Gbps”. Estas instancias tienen una banda ancha de base. Para satisfacer la demanda adicional, pueden utilizar un mecanismo de créditos de E/S de red para superar la banda ancha de base. Las instancias pueden utilizar la banda ancha de fragmentación durante un tiempo limitado, normalmente de 5 a 60 minutos, en función del tamaño de la instancia.

Una instancia recibe el número máximo de créditos de E/S de red en el momento de la inicialización. Si la instancia agota sus créditos de E/S de red, vuelve a su banda ancha de base. Una instancia en ejecución obtiene créditos de E/S de red cada vez que utiliza menos banda ancha de red que su banda ancha de base. Una instancia detenida no gana créditos de E/S de red. La ráfaga de instancia se basa en el mejor esfuerzo, incluso cuando la instancia tiene créditos disponibles, ya que la banda ancha de ráfaga es un recurso compartido.

Hay buckets de créditos de E/S de red independientes para el tráfico entrante y saliente.

Rendimiento de red base y ráfaga

La Guía de tipos de instancias de Amazon EC2 describe el rendimiento de red para cada tipo de instancia, además del ancho de banda de la red de referencia disponible para las instancias que pueden utilizar un ancho de banda ampliado. Para más información, consulte los siguientes temas:

- Especificaciones de red: uso general
- Especificaciones de red: optimizadas para computación
- Especificaciones de red: memoria optimizada
- Especificaciones de red: almacenamiento optimizado
- Especificaciones de red: computación acelerada
- Especificaciones de red: computación de alto rendimiento
- Especificaciones de red: generación anterior

Para ver el rendimiento de la red mediante la herramienta AWS CLI

Puede utilizar el comando describe-instance-types de la AWS CLIpara mostrar información sobre un tipo de instancias. En el siguiente ejemplo se muestra información sobre el rendimiento de la red para todas las instancias C5.

```
aws ec2 describe-instance-types --filters "Name=instance-type,Values=c5.*"
 --query "InstanceTypes[].[InstanceType, NetworkInfo.NetworkPerformance,
 NetworkInfo.NetworkCards[0].BaselineBandwidthInGbps]" --output table
-------------------------------------------
|           DescribeInstanceTypes           |
+--------------+--------------------+-------+
|  c5.4xlarge  |  Up to 10 Gigabit  |  5.0  |
|  c5.xlarge   |  Up to 10 Gigabit  |  1.25 |
|  c5.12xlarge |  12 Gigabit        |  12.0 |
|  c5.24xlarge |  25 Gigabit        |  25.0 |
|  c5.metal    |  25 Gigabit        |  25.0 |
|  c5.9xlarge  |  12 Gigabit        |  12.0 |
|  c5.2xlarge  |  Up to 10 Gigabit  |  2.5  |
|  c5.large    |  Up to 10 Gigabit  |  0.75 |
|  c5.18xlarge |  25 Gigabit        |  25.0 |
+--------------+--------------------+-------+
```

Monitoreo del ancho de banda de las instancias

Puede usar las métricas de CloudWatch para monitorear el ancho de banda de red de las instancias y los paquetes enviados y recibidos. Puede utilizar las métricas de rendimiento de red proporcionadas por el controlador de Elastic Network Adapter (ENA) para monitorear cuándo el tráfico supera los límites de red que Amazon EC2 define en el nivel de instancia.

Puede configurar si Amazon EC2 envía datos de métricas de la instancia a CloudWatch utilizando periodos de un minuto o periodos de cinco minutos. Es posible que las métricas de rendimiento de red muestren que se ha superado un límite y se han eliminado los paquetes, mientras que las métricas de instancias de CloudWatch no lo hacen. Esto puede ocurrir cuando la instancia tiene un pico corto en la demanda de recursos de red (conocido como microampliación), pero las métricas de CloudWatch no son lo suficientemente pormenorizadas como para reflejar estos picos de microsegundos.

Más información

- Métricas de la instancia
- Métricas de rendimiento de la red

Redes mejoradas en Amazon EC2

Las redes mejoradas utilizan la virtualización de E/S de raíz única (SR-IOV) para ofrecer funcionalidades de redes de alto rendimiento en los tipos de instancias soportados. SR-IOV es un método de virtualización de dispositivos que ofrece un mayor rendimiento de E/S y una menor utilización de CPU en comparación con las interfaces de red virtualizadas tradicionales. Las redes mejoradas proporcionan un mayor ancho de banda, un rendimiento superior de paquetes por segundo (PPS) y menores latencias entre instancias de manera constante. El uso de las redes mejoradas no supone ningún cargo adicional.

Para obtener más información sobre la velocidad de red admitida para cada tipo de instancia, consulte los Tipos de instancia de Amazon EC2.

Contenido

Se ha mejorado la compatibilidad de red

Todos los tipos de instancias de la generación actual admiten redes mejoradas, excepto las instancias T2.

Puede habilitar redes mejoradas mediante uno de los siguientes mecanismos:

Elastic Network Adapter (ENA)

> Elastic Network Adapter (ENA) admite velocidades de red de hasta 100 Gbps en los tipos de instancias admitidos.

Todas las instancias integradas en el AWS Nitro System utilizan ENA para mejorar la conexión en red. Además, los siguientes tipos de instancias Xen admiten ENA: H1, G3, `m4.16xlarge`, P2, P3, P3dn y R4.

Para obtener más información, consulte Habilitación de las redes mejoradas con Elastic Network Adapter (ENA) en las instancias EC2.

Interfaz de Intel 82599 Virtual Function (VF)

La interfaz de Intel 82599 Virtual Function admite velocidades de red de hasta 10 Gbps en los tipos de instancias soportados.

Los siguientes tipos de instancia utilizan la interfaz Intel 82599 VF para redes mejoradas: C3, C4, D2, I2, M4 (excepto m4.16xlarge) y R3.

Para obtener más información, consulte Habilitación de redes mejoradas con la interfaz de Intel 82599 VF en instancias EC2.

Habilitación de las redes mejoradas con Elastic Network Adapter (ENA) en las instancias EC2

Amazon EC2 proporciona funcionalidades de redes mejoradas a través del Elastic Network Adapter (ENA). Para utilizar la conexión en red mejorada, debe instalar el módulo ENA requerido y habilitar la compatibilidad con ENA.

Contenido

Requisitos

Para prepararse para las redes mejoradas con ENA, configure la instancia de la siguiente manera:

- Inicialice una instancia basada en AWS Nitro System.
- Asegúrese de que la instancia tenga conexión a Internet.
- Si tiene datos importantes en la instancia que desea conservar, debería realizar ahora una copia de seguridad de esos datos creando una AMI desde la instancia. La actualización del kernel y los módulos del kernel, además de habilitar el atributo `enaSupport`, puede hacer que las instancias o sistemas operativos incompatibles sean inaccesibles. Si tiene una copia de seguridad reciente y esto ocurre, los datos se conservarán.
- Instancias de Linux: lance una instancia con una versión del kernel de Linux y una distribución admitidas, de manera que la red mejorada de ENA esté habilitada de forma automática para su instancia. Para obtener más información, consulte ENA Linux Kernel Driver Release Notes.
- Instancias de Windows: si la instancia ejecuta Windows Server 2008 R2 SP1, asegúrese de que tiene la actualización de compatibilidad con firma de código SHA-2.
- Utilice AWS CloudShell en la AWS Management Console, o bien instale y configure la AWS CLI o las AWS Tools for Windows PowerShell en cualquier computadora que elija, preferentemente en su equipo de escritorio o portátil local. Para obtener más información, consulte Acceder a Amazon EC2 o la Guía del usuario de AWS CloudShell. Las redes mejoradas no se pueden administrar desde la consola de Amazon EC2.

Rendimiento de red mejorado

La documentación siguiente proporciona un resumen del rendimiento de la red para los tipos de instancia que admiten redes mejoradas ENA:

- Especificaciones de red para instancias de computación acelerada
- Especificaciones de red para instancias optimizadas para la computación
- Especificaciones de red para instancias de uso general
- Especificaciones de red para instancias de computación de alto rendimiento
- Especificaciones de red para instancias optimizadas para memoria
- Especificaciones de red para instancias optimizadas para el almacenamiento

AMI de Linux con el módulo requerido

Las siguientes AMI incluyen el módulo ENA requerido y tienen habilitada la compatibilidad con ENA:

- AL2023

- Amazon Linux 2
- AMI de Amazon Linux 2018.03 y posterior
- Ubuntu 14.04 o versiones posteriores con el kernel `linux-aws`

> **Note**
>
> Los tipos de instancias basados en AWS Graviton requieren Ubuntu 18.04 o versiones posteriores con kernel `linux-aws`

- Red Hat Enterprise Linux 7.4 o versiones posteriores
- SUSE Linux Enterprise Server 12 SP2 o versiones posteriores
- CentOS 7.4.1708 o versiones posteriores
- FreeBSD 11.1 o versiones posteriores
- Debian GNU/Linux 9 o versiones posteriores

Para probar si la conexión en red mejorada ya está habilitada, compruebe que el módulo `ena` esté instalado en la instancia y que se haya establecido el atributo `enaSupport`. De ser así, el comando ethtool -i eth*n* debería mostrar que el módulo se está utilizando en la interfaz de red.

Módulo de kernel (ena)

Para comprobar si el módulo `ena` está instalado, utilice el comando modinfo como se indica en el siguiente ejemplo.

```
[ec2-user ~]$ modinfo ena
filename:    /lib/modules/4.14.33-59.37.amzn2.x86_64/kernel/drivers/amazon/net/ena/
ena.ko
version:  1.5.0g
license:  GPL
description: Elastic Network Adapter (ENA)
author:   Amazon.com, Inc. or its affiliates
srcversion:  692C7C68B8A9001CB3F31D0
alias:    pci:v00001D0Fd0000EC21sv*sd*bc*sc*i*
alias:    pci:v00001D0Fd0000EC20sv*sd*bc*sc*i*
alias:    pci:v00001D0Fd00001EC2sv*sd*bc*sc*i*
alias:    pci:v00001D0Fd00000EC2sv*sd*bc*sc*i*
depends:
retpoline:   Y
```

```
intree:   Y
name:     ena
...
```

En la instancia de Amazon Linux, el módulo `ena` está instalado.

```
ubuntu:~$ modinfo ena
ERROR: modinfo: could not find module ena
```

En la instancia de Ubuntu, el módulo no está instalado, por lo que debe instalarlo primero. Para obtener más información, consulte Ubuntu.

Probar si las redes mejoradas están habilitadas

Puede probar si las redes mejoradas están habilitadas en las instancias o AMI.

Atributo de instancia

Para comprobar si una instancia tiene establecido el atributo `enaSupport` de las redes mejoradas, utilice uno de los siguientes comandos. Si el atributo está establecido, la respuesta es true.

- describe-instances (AWS CLI/AWS CloudShell)

```
aws ec2 describe-instances --instance-ids instance_id --query
 "Reservations[].Instances[].EnaSupport"
```

- Get-EC2Instance (Herramientas para Windows PowerShell)

```
(Get-EC2Instance -InstanceId instance-id).Instances.EnaSupport
```

Atributo de imagen

Para comprobar si una AMI tiene establecido el atributo `enaSupport` de las redes mejoradas, utilice uno de los siguientes comandos. Si el atributo está establecido, la respuesta es true.

- describe-images (AWS CLI/AWS CloudShell)

```
aws ec2 describe-images --image-id ami_id --query "Images[].EnaSupport"
```

- Get-EC2Image (Herramientas para Windows PowerShell)

```
(Get-EC2Image -ImageId ami_id).EnaSupport
```

Controlador de la interfaz de red de Linux

Utilice el siguiente comando para verificar si el módulo `ena` se está utilizando en una interfaz en particular, sustituyendo el nombre de la interfaz que quiere comprobar. Si utiliza una sola interfaz (predeterminada), esta será `eth0`. Si el sistema operativo admite nombres de red predecibles, podría ser un nombre como `ens5`.

En el ejemplo siguiente, el módulo `ena` no está cargado, ya que el controlador indicado es `vif`.

```
[ec2-user ~]$ ethtool -i eth0
driver: vif
version:
firmware-version:
bus-info: vif-0
supports-statistics: yes
supports-test: no
supports-eeprom-access: no
supports-register-dump: no
supports-priv-flags: no
```

En este ejemplo, el módulo `ena` está cargado y tiene la versión mínima recomendada. Esta instancia tiene las redes mejoradas configuradas correctamente.

```
[ec2-user ~]$ ethtool -i eth0
driver: ena
version: 1.5.0g
firmware-version:
expansion-rom-version:
bus-info: 0000:00:05.0
supports-statistics: yes
supports-test: no
supports-eeprom-access: no
supports-register-dump: no
supports-priv-flags: no
```

Habilitar redes mejoradas en la instancia

El procedimiento que utiliza depende del sistema operativo de la instancia.

Amazon Linux

Amazon Linux 2 y las últimas versiones de la Amazon Linux AMI incluyen el módulo requerido para mejorar la conexión en red con ENA instalado y tienen habilitada la compatibilidad con ENA. Por lo tanto, si inicia una instancia con una versión HVM de Amazon Linux en un tipo de instancia admitido, las redes mejoradas ya están habilitadas para su instancia. Para obtener más información, consulte Probar si las redes mejoradas están habilitadas.

Si ha iniciado la instancia utilizando una AMI de Amazon Linux más antigua y no tiene habilitadas aún las redes mejoradas, utilice el siguiente procedimiento para habilitarlas.

Para habilitar las redes mejoradas en Amazon Linux AMI

1. Conéctese a la instancia.
2. Desde la instancia, ejecute el siguiente comando para actualizarla con el kernel y los módulos de kernel más recientes, incluido `ena`:

   ```
   [ec2-user ~]$ sudo yum update
   ```
3. Desde su equipo local, reinicie la instancia mediante la consola de Amazon EC2 o uno de los siguientes comandos: reboot-instances (AWS CLI), Restart-EC2Instance (AWS Tools for Windows PowerShell).
4. Conéctese de nuevo a la instancia y compruebe si el módulo `ena` está instalado y si tiene la versión mínima recomendada utilizando el comando modinfo ena de Probar si las redes mejoradas están habilitadas.
5. [instancia basada en EBS] Desde su equipo local, detenga la instancia mediante la consola de Amazon EC2 o uno de los siguientes comandos: stop-instances (AWS CLI), Stop-EC2Instance (AWS Tools for Windows PowerShell). Si la instancia la administra AWS OpsWorks, debe detenerla en la consola de AWS OpsWorks para mantener su estado sincronizado.

   [Instancia respaldada por el almacén de instancias] No puede detener la instancia para modificar el atributo. En lugar de ello, vaya a este procedimiento: Para habilitar las redes mejoradas en Amazon Linux AMI (instancias con el respaldado del almacén de instancias).
6. En el equipo local, habilite el atributo de redes mejoradas con uno de los siguientes comandos:

   - modify-instance-attribute (AWS CLI)

     ```
     aws ec2 modify-instance-attribute --instance-id instance_id --ena-support
     ```

- Edit-EC2InstanceAttribute (Herramientas para Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId instance-id -EnaSupport $true
```

7. (Opcional) Cree una AMI desde la instancia, tal y como se explica en Creación de una AMI basada en Amazon EBS. La AMI hereda el atributo de redes mejoradas `enaSupport` de la instancia. Por lo tanto, puede utilizar esta AMI para iniciar otra instancia con las redes mejoradas habilitadas de manera predeterminada.
8. Desde su equipo local, inicie la instancia mediante la consola de Amazon EC2 o uno de los siguientes comandos: start-instances (AWS CLI), Start-EC2Instance (AWS Tools for Windows PowerShell). Si la instancia la administra AWS OpsWorks, debe iniciarla en la consola de AWS OpsWorks para mantener su estado sincronizado.
9. Conéctese a la instancia y compruebe que el módulo `ena` está instalado y cargado en la interfaz de red utilizando el comando ethtool -i eth*n* command de Probar si las redes mejoradas están habilitadas.

   Si no puede conectarse a la instancia después de habilitar las redes mejoradas, consulte Solución de problemas de Elastic Network Adapter en Linux.

Para habilitar las redes mejoradas en Amazon Linux AMI (instancias con el respaldado del almacén de instancias)

Siga el procedimiento anterior hasta el paso en el que detiene la instancia. Cree una nueva AMI tal como se describe en Crear una AMI de Linux con respaldo en el almacén de instancias, asegurándose de habilitar el atributo de redes mejoradas cuando registre la AMI.

- register-image (AWS CLI)

```
aws ec2 register-image --ena-support ...
```

- Register-EC2Image (AWS Tools for Windows PowerShell)

```
Register-EC2Image -EnaSupport $true ...
```

Ubuntu

Las últimas AMI de Ubuntu HVM incluyen el módulo requerido para mejorar la conexión en red con ENA instalado y tienen habilitada la compatibilidad con ENA. Por lo tanto, si inicia una instancia con la AMI HVM de Ubuntu más reciente en un tipo de instancia admitido, las redes mejoradas ya están habilitadas para su instancia. Para obtener más información, consulte Probar si las redes mejoradas están habilitadas.

Si ha iniciado la instancia utilizando una AMI más antigua que no tiene habilitada aún la conexión en red mejorada, puede instalar el paquete del kernel `linux-aws` para obtener los controladores de red mejorada más recientes y actualizar el atributo necesario.

Para instalar el paquete del kernel de **`linux-aws`** (Ubuntu 16.04 o versiones posteriores)

Ubuntu 16.04 y 18.04 se distribuyen con el kernel personalizado de Ubuntu (paquete del kernel de `linux-aws`). Para usar un kernel diferente, contacte con AWS Support.

Para instalar el paquete del kernel de **`linux-aws`** (Ubuntu Trusty 14.04)

1. Conéctese a la instancia.
2. Actualice la caché del paquete y los paquetes.

```
ubuntu:~$ sudo apt-get update && sudo apt-get upgrade -y linux-aws
```

> **Important**
>
> Si, durante el proceso de actualización, se le pide que instale `grub`, use `/dev/xvda` para instalar `grub` y luego elija conservar la versión actual de `/boot/grub/menu.lst`.

3. [instancia basada en EBS] Desde su equipo local, detenga la instancia mediante la consola de Amazon EC2 o uno de los siguientes comandos: stop-instances (AWS CLI), Stop-EC2Instance (AWS Tools for Windows PowerShell). Si la instancia la administra AWS OpsWorks, debe detenerla en la consola de AWS OpsWorks para mantener su estado sincronizado.

   [Instancia respaldada por el almacén de instancias] No puede detener la instancia para modificar el atributo. En lugar de ello, vaya a este procedimiento: Para habilitar las redes mejoradas en Ubuntu (instancias con respaldo en el almacén de instancias).
4. En el equipo local, habilite el atributo de redes mejoradas con uno de los siguientes comandos:

- modify-instance-attribute (AWS CLI)

```
aws ec2 modify-instance-attribute --instance-id instance_id --ena-support
```

- Edit-EC2InstanceAttribute (Herramientas para Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId instance-id -EnaSupport $true
```

5. (Opcional) Cree una AMI desde la instancia, tal y como se explica en Creación de una AMI basada en Amazon EBS. La AMI hereda el atributo de redes mejoradas `enaSupport` de la instancia. Por lo tanto, puede utilizar esta AMI para iniciar otra instancia con las redes mejoradas habilitadas de manera predeterminada.
6. Desde su equipo local, inicie la instancia mediante la consola de Amazon EC2 o uno de los siguientes comandos: start-instances (AWS CLI), Start-EC2Instance (AWS Tools for Windows PowerShell). Si la instancia la administra AWS OpsWorks, debe iniciarla en la consola de AWS OpsWorks para mantener su estado sincronizado.

Para habilitar las redes mejoradas en Ubuntu (instancias con respaldo en el almacén de instancias)

Siga el procedimiento anterior hasta el paso en el que detiene la instancia. Cree una nueva AMI tal como se describe en Crear una AMI de Linux con respaldo en el almacén de instancias, asegurándose de habilitar el atributo de redes mejoradas cuando registre la AMI.

- register-image (AWS CLI)

```
aws ec2 register-image --ena-support ...
```

- Register-EC2Image (AWS Tools for Windows PowerShell)

```
Register-EC2Image -EnaSupport $true ...
```

RHEL, SUSE, CentOS

Las últimas AMI de Red Hat Enterprise Linux, SUSE Linux Enterprise Server y CentOS incluyen el módulo requerido para mejorar la conexión en red con ENA y tienen habilitada la compatibilidad con ENA. Por lo tanto, si inicia una instancia con la AMI más reciente en un tipo de instancia admitido,

la conexión en red mejorada ya está habilitada para su instancia. Para obtener más información, consulte Probar si las redes mejoradas están habilitadas.

En el siguiente procedimiento, se proporcionan los pasos para habilitar la conexión en red mejorada con ENA en una distribución de Linux distinta de Amazon Linux AMI o Ubuntu. Para obtener más información, como la sintaxis detallada de los comandos, las ubicaciones de los archivos o la compatibilidad con paquetes y herramientas, consulte la documentación de su distribución de Linux.

Para habilitar las redes mejoradas en Linux

1. Conéctese a la instancia.
2. Clone el código fuente para el módulo `ena` en la instancia desde GitHub en https://github.com/amzn/amzn-drivers. (SUSE Linux Enterprise Server 12 SP2 y versiones posteriores incluyen ENA 2.02 de forma predeterminada, por lo que no es necesario descargar ni compilar el controlador de ENA. Para SUSE Linux Enterprise Server 12 SP2 y versiones posteriores, debe tramitar una solicitud para agregar la versión del controlador que desee al kernel existente).

   ```
   git clone https://github.com/amzn/amzn-drivers
   ```

3. Compile e instale el módulo `ena` en la instancia. Estos pasos dependen de la distribución Linux. Para obtener más información sobre la compilación del módulo en Red Hat Enterprise Linux, consulte ¿Cómo puedo instalar y activar el controlador ENA más reciente para mejorar la compatibilidad de red en una instancia de Amazon EC2 que ejecuta RHEL?
4. Ejecute el comando sudo depmod para actualizar las dependencias de módulos.
5. Actualice `initramfs` en la instancia para asegurarse de que el nuevo módulo se carga en el momento del arranque. Por ejemplo, si su distribución admite dracut, puede utilizar el comando siguiente.

   ```
   dracut -f -v
   ```

6. Determine si el sistema utiliza de manera predeterminada nombres de interfaz de red predecibles. Los sistemas que utilizan las versiones 197 o posteriores de systemd o udev pueden cambiar el nombre de los dispositivos Ethernet y no garantizan que haya una sola interfaz de red denominada `eth0`. Este comportamiento puede producir problemas al conectarse a la instancia. Para obtener más información y para ver otras opciones de configuración, consulte Predictable Network Interface Names en el sitio web de freedesktop.org.

a. Puede utilizar el siguiente comando para comprobar las versiones de systemd o udev en los sistemas basados en RPM.

```
rpm -qa | grep -e '^systemd-[0-9]\+\|^udev-[0-9]\+'
systemd-208-11.el7_0.2.x86_64
```

En el ejemplo anterior de Red Hat Enterprise Linux 7, la versión de systemd es la 208, por lo que se deben deshabilitar los nombres de interfaz de red predecibles.

b. Para deshabilitar los nombres de interfaz de red predecibles, añada la opción `net.ifnames=0` a la línea `GRUB_CMDLINE_LINUX` en `/etc/default/grub`.

```
sudo sed -i '/^GRUB\_CMDLINE\_LINUX/s/\"$/\ net\.ifnames\=0\"/' /etc/default/
grub
```

c. Vuelva a compilar el archivo de configuración de Grub.

```
sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

7. [instancia basada en EBS] Desde su equipo local, detenga la instancia mediante la consola de Amazon EC2 o uno de los siguientes comandos: stop-instances (AWS CLI), Stop-EC2Instance (AWS Tools for Windows PowerShell). Si la instancia la administra AWS OpsWorks, debe detenerla en la consola de AWS OpsWorks para mantener su estado sincronizado.

   [Instancia respaldada por el almacén de instancias] No puede detener la instancia para modificar el atributo. En lugar de ello, vaya a este procedimiento: Para habilitar las redes mejoradas en Linux (instancias respaldadas por el almacén de instancias).

8. En el equipo local, habilite el atributo `enaSupport` de redes mejoradas con uno de los siguientes comandos:

   - modify-instance-attribute (AWS CLI)

   ```
   aws ec2 modify-instance-attribute --instance-id instance_id --ena-support
   ```

   - Edit-EC2InstanceAttribute (Herramientas para Windows PowerShell)

   ```
   Edit-EC2InstanceAttribute -InstanceId instance-id -EnaSupport $true
   ```

9. (Opcional) Cree una AMI desde la instancia, tal y como se explica en Creación de una AMI basada en Amazon EBS. La AMI hereda el atributo de redes mejoradas `enaSupport` de la instancia. Por lo tanto, puede utilizar esta AMI para iniciar otra instancia con las redes mejoradas habilitadas de manera predeterminada.

   Si el sistema operativo de la instancia contiene un archivo `/etc/udev/rules.d/70-persistent-net.rules`, debe eliminarlo antes de crear la AMI. Este archivo contiene la dirección MAC del adaptador Ethernet de la instancia original. Si otra instancia arranca con este archivo, el sistema operativo no será capaz de encontrar el dispositivo y `eth0` producirá un error, lo que causará problemas de arranque. Este archivo se regenera en el siguiente ciclo de arranque y todas las instancias que se inician desde la AMI crean su propia versión del archivo.
10. Desde su equipo local, inicie la instancia mediante la consola de Amazon EC2 o uno de los siguientes comandos: start-instances (AWS CLI), Start-EC2Instance (AWS Tools for Windows PowerShell). Si la instancia la administra AWS OpsWorks, debe iniciarla en la consola de AWS OpsWorks para mantener su estado sincronizado.
11. (Opcional) Conéctese a la instancia y compruebe si el módulo está instalado.

    Si no puede conectarse a la instancia después de habilitar las redes mejoradas, consulte Solución de problemas de Elastic Network Adapter en Linux.

Para habilitar las redes mejoradas en Linux (instancias respaldadas por el almacén de instancias)

Siga el procedimiento anterior hasta el paso en el que detiene la instancia. Cree una nueva AMI tal como se describe en Crear una AMI de Linux con respaldo en el almacén de instancias, asegurándose de habilitar el atributo de redes mejoradas cuando registre la AMI.

- register-image (AWS CLI)

```
aws ec2 register-image --ena-support ...
```

- Register-EC2Image (AWS Tools for Windows PowerShell)

```
Register-EC2Image -EnaSupport ...
```

Ubuntu con DKMS

Este método sirve únicamente para realizar pruebas y enviar comentarios. No se ha concebido para su uso en implementaciones de producción. Para las implementaciones de producción, consulte Ubuntu.

> **Important**
>
> El uso de DKMS invalida el acuerdo de soporte técnico de su suscripción. No se debe usar para implementaciones de producción.

Para habilitar las redes mejoradas con ENA en Ubuntu (instancias con respaldo de EBS)

1. Siga los pasos 1 y 2 de Ubuntu.
2. Instale los paquetes `build-essential` para compilar el módulo del kernel y el paquete `dkms` para volver a compilar el módulo `ena` cada vez que se actualiza el kernel.

   ```
   ubuntu:~$ sudo apt-get install -y build-essential dkms
   ```

3. Clone el código fuente del módulo `ena` en la instancia desde GitHub en https://github.com/amzn/amzn-drivers.

   ```
   ubuntu:~$ git clone https://github.com/amzn/amzn-drivers
   ```

4. Mueva el paquete `amzn-drivers` al directorio `/usr/src/` para que DKMS pueda encontrarlo y compilarlo en cada actualización del kernel. Añada el número de versión (lo encontrará en las notas de la versión) del código fuente al nombre del directorio. Por ejemplo, en el ejemplo siguiente se muestra la versión `1.0.0`.

   ```
   ubuntu:~$ sudo mv amzn-drivers /usr/src/amzn-drivers-1.0.0
   ```

5. Cree el archivo de configuración DKMS con los siguientes valores, sustituyendo su versión de `ena`.

   Cree el archivo.

   ```
   ubuntu:~$ sudo touch /usr/src/amzn-drivers-1.0.0/dkms.conf
   ```

Edite el archivo y añada los valores siguientes.

```
ubuntu:~$ sudo vim /usr/src/amzn-drivers-1.0.0/dkms.conf
PACKAGE_NAME="ena"
PACKAGE_VERSION="1.0.0"
CLEAN="make -C kernel/linux/ena clean"
MAKE="make -C kernel/linux/ena/ BUILD_KERNEL=${kernelver}"
BUILT_MODULE_NAME[0]="ena"
BUILT_MODULE_LOCATION="kernel/linux/ena"
DEST_MODULE_LOCATION[0]="/updates"
DEST_MODULE_NAME[0]="ena"
AUTOINSTALL="yes"
```

6. Añada, compile e instale el módulo `ena` en su instancia utilizando DKMS.

   Añada el módulo a DKMS.

   ```
   ubuntu:~$ sudo dkms add -m amzn-drivers -v 1.0.0
   ```

   Compile el módulo utilizando el comando dkms.

   ```
   ubuntu:~$ sudo dkms build -m amzn-drivers -v 1.0.0
   ```

   Instale el módulo utilizando dkms.

   ```
   ubuntu:~$ sudo dkms install -m amzn-drivers -v 1.0.0
   ```

7. Vuelva a compilar `initramfs` para que el módulo correcto se cargue en el momento del arranque.

   ```
   ubuntu:~$ sudo update-initramfs -u -k all
   ```

8. Compruebe si el módulo `ena` está instalado utilizando el comando modinfo ena desde Probar si las redes mejoradas están habilitadas.

   ```
   ubuntu:~$ modinfo ena
   filename:    /lib/modules/3.13.0-74-generic/updates/dkms/ena.ko
   version:  1.0.0
   license:  GPL
   description: Elastic Network Adapter (ENA)
   ```

```
author:   Amazon.com, Inc. or its affiliates
srcversion:  9693C876C54CA64AE48F0CA
alias:    pci:v00001D0Fd0000EC21sv*sd*bc*sc*i*
alias:    pci:v00001D0Fd0000EC20sv*sd*bc*sc*i*
alias:    pci:v00001D0Fd00001EC2sv*sd*bc*sc*i*
alias:    pci:v00001D0Fd00000EC2sv*sd*bc*sc*i*
depends:
vermagic:    3.13.0-74-generic SMP mod_unload modversions
parm:     debug:Debug level (0=none,...,16=all) (int)
parm:     push_mode:Descriptor / header push mode (0=automatic,1=disable,3=enable)
     0 - Automatically choose according to device capability (default)
     1 - Don't push anything to device memory
     3 - Push descriptors and header buffer to device memory (int)
parm:     enable_wd:Enable keepalive watchdog (0=disable,1=enable,default=1) (int)
parm:     enable_missing_tx_detection:Enable missing Tx completions. (default=1)
 (int)
parm:     numa_node_override_array:Numa node override map
 (array of int)
parm:     numa_node_override:Enable/Disable numa node override (0=disable)
 (int)
```

9. Continúe con el paso 3 de Ubuntu.

Habilitar redes mejoradas en Windows

Si ha iniciado su instancia y no tiene habilitadas aún las redes mejoradas, debe descargar e instalar el controlador del adaptador de red requerido en la instancia y luego establecer el atributo de la instancia `enaSupport` para activar las redes mejoradas. Solo puede habilitar este atributo en los tipos de instancias admitidos y solo si está instalado el controlador de ENA. Para obtener más información, consulte Se ha mejorado la compatibilidad de red.

Para habilitar las redes mejoradas

1. Conéctese a la instancia e inicie sesión como administrador local.
2. [Windows Server 2016 y 2019 únicamente] Ejecute el siguiente script de PowerShell de EC2Launch para configurar la instancia después de instalar el controlador.

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
Schedule
```

3. En la instancia, instale el controlador de la siguiente manera:

a. Descargue el controlador más reciente en la instancia.

b. Extraiga el archivo zip.

c. Instale el controlador ejecutando el script de PowerShell `install.ps1`.

> **Note**
>
> Si recibe un error de política de ejecución, establezca la política en `Unrestricted` (el valor predeterminado es `Restricted` o `RemoteSigned`). En una línea de comandos, ejecute `Set-ExecutionPolicy -ExecutionPolicy Unrestricted` y, a continuación, ejecute de nuevo el script `install.ps1` de PowerShell.

4. Desde su equipo local, detenga la instancia mediante la consola de Amazon EC2 o uno de los siguientes comandos: stop-instances (AWS CLI/AWS CloudShell), Stop-EC2Instance (AWS Tools for Windows PowerShell). Si la instancia la administra AWS OpsWorks, debe detenerla en la consola de AWS OpsWorks para mantener su estado sincronizado.

5. Habilite el soporte de ENA en la instancia del modo siguiente:

   a. En el equipo local, compruebe el atributo de soporte de ENA de la instancia de EC2 en la instancia ejecutando uno de los siguientes comandos. Si el atributo no está habilitado, la salida será "[]" o estará en blanco. `EnaSupport` está establecido en `false` de forma predeterminada.

   - describe-instances (AWS CLI/AWS CloudShell)

```
aws ec2 describe-instances --instance-ids instance_id --query
 "Reservations[].Instances[].EnaSupport"
```

   - Get-EC2Instance (Herramientas para Windows PowerShell)

```
(Get-EC2Instance -InstanceId instance-id).Instances.EnaSupport
```

   b. Para habilitar el soporte de ENA, ejecute uno de los siguientes comandos:

   - modify-instance-attribute (AWS CLI/AWS CloudShell)

```
aws ec2 modify-instance-attribute --instance-id instance_id --ena-support
```

- Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId instance_id -EnaSupport $true
```

Si tiene problemas al reiniciar la instancia, también puede deshabilitar el soporte de ENA con uno de los siguientes comandos:

- modify-instance-attribute (AWS CLI/AWS CloudShell)

```
aws ec2 modify-instance-attribute --instance-id instance_id --no-ena-support
```

- Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId instance_id -EnaSupport $false
```

c. Verifique que el atributo se ha establecido en `true` usando describe-instances o Get-EC2Instance como se ha explicado antes. Entonces, debe ver la salida siguiente:

```
[
 true
]
```

6. Desde su equipo local, inicie la instancia mediante la consola de Amazon EC2 o uno de los siguientes comandos: start-instances (AWS CLI/AWS CloudShell), Start-EC2Instance (AWS Tools for Windows PowerShell). Si la instancia la administra AWS OpsWorks, debe iniciarla con la consola de AWS OpsWorks para que su estado se mantenga sincronizado.
7. En la instancia, confirme que el controlador de ENA esté instalado y habilitado del modo siguiente:

   a. Haga clic con el botón derecho en el icono de red y elija Abrir el centro de redes y recursos compartidos.

   b. Elija el adaptador Ethernet (por ejemplo, Ethernet 2).

   c. Elija Detalles. En Detalles de la conexión de red, compruebe que Descripción tiene el valor Amazon Elastic Network Adapter.

8. (Opcional) Cree una AMI a partir de la instancia. La AMI hereda el atributo `enaSupport` de la instancia. Por lo tanto, puede utilizar esta AMI para iniciar otra instancia con ENA habilitado de manera predeterminada.

Notas de versión del controlador

Controlador de ENA de Linux

Para obtener información acerca de las versiones del controlador de ENA de Linux, consulte las notas de la versión del controlador del kernel de ENA de Linux.

Controlador de ENA de Windows

Las AMI para Windows incluyen el controlador de Amazon ENA para habilitar las redes mejoradas.

La siguiente tabla muestra la versión del controlador ENA correspondiente que se debe descargar para cada versión de Windows Server.

Versión de Windows Server	Versión del controlador ENA
Windows Server 2022	2.4.0 y versiones posteriores
Windows Server 2019	más recientes
Windows Server 2016	más recientes
Windows Server 2012 R2	2.6.0 y versiones anteriores
Windows Server 2012	2.6.0 y versiones anteriores
Windows Server 2008 R2	2.2.3 y versiones posteriores

En la tabla siguiente se resumen los cambios de cada versión.

Versión de controlador	Detalles	Fecha de la versión
2.7.0	Nuevas características • Se eliminó la compatibilidad con Windows Server 2012 (Windows 8) y Windows Server 2012 R2	1 de mayo de 2024

Versión de controlador	Detalles	Fecha de la versión
	(Windows 8.1). La compatibilidad de AWS con estas versiones de sistemas operativos finalizó. La instalación del controlador fallará en Windows Server 2012 y versiones anteriores. • Se agregó compatibilidad con la transferencia del cálculo de la suma de verificación de IPv6 Tx al dispositivo. • Se agregó una amplia compatibilidad con colas de baja latencia (LLQ). Esto se activa de forma dinámica según las recomendaciones del dispositivo. Puede anular esta configuración con la nueva clave de registro “WideLLQ” . • Se agregó un informe sobre las pérdidas de paquetes provocadas por un exceso de Rx, lo que indica que no hay suficiente espacio en el anillo Rx para los paquetes entrantes. • Se agregó compatibilidad para las notificaciones de configuración subóptimas desde el dispositivo. Consulte el ID del evento `59000` desde el lector de eventos de Windows. Correcciones de errores • Evite el reinicio de dispositivos innecesario causado por los paquetes Tx con encabezados que excedan el tamaño de encabezado máximo de las colas de baja latencia (LLQ).	

Versión de controlador	Detalles	Fecha de la versión

2.6.0	Nuevas características
	• Agrega las siguientes métricas de rendimiento de red para los tipos de instancias compatibles con ENA Express.
	  • `ena_srd_mode`
	  • `ena_srd_tx_pkts`
	  • `ena_srd_eligible_tx_pkts`
	  • `ena_srd_rx_pkts`
	  • `ena_srd_resource_utilization`
	• Agrega la métrica de rendimiento de red `conntrack_allowance_available` para los tipos de instancias basados en Nitro.
	• Agrega un nuevo motivo para restablecer el adaptador debido a la detección de daños en los datos de RX.
	• Actualiza la infraestructura de registro de controladores.
	
	Correcciones de errores
	• Impide el restablecimiento del adaptador en caso de que la falta de CPU provoque un error en la actualización de las métricas de rendimiento de red.
	•
		20 de junio de 2023

Versión de controlador	Detalles	Fecha de la versión
	Impide la detección falsa de una interrupción del ritmo cardíaco del dispositivo. • Corrige el script de instalación del controlador para permitir la operación de adopción de una versión anterior. • Corrige la estadística de recuento de errores de recepción.	
2.5.0	Anuncio La versión 2.5.0 del controlador ENA Windows se revirtió debido a un fallo de inicialización en el controlador de dominio de Windows. Windows Client y Windows Server no están afectados.	17 de febrero de 2023

Versión de controlador	Detalles	Fecha de la versión
2.4.0	Nuevas características • Agrega compatibilidad con Windows Server 2022 • Elimina compatibilidad con Windows Server 2008 R2. • Establece la cola de baja latencia (LLQ) para que siempre esté activada con el fin de mejorar el rendimiento de las instancias de Amazon EC2 de sexta generación. Corrección de errores • Corrige un error al publicar métricas de rendimiento de red en el sistema de contadores de rendimiento para Windows (PCW). • Corrige una pérdida de memoria durante la operación de lectura de claves del registro. • Evita la creación de un bucle de restablecimiento infinito en caso de que se produzca un error irrecuper able durante el proceso de restablecimiento del adaptador.	28 de abril de 2022

Versión de controlador	Detalles	Fecha de la versión

2.2.4	Anuncios
	
	La versión 2.2.4 del controlador ENA Windows se revirtió debido a la posible disminución del rendimiento en las instancias de EC2 de sexta generación. Recomendamos que cambie a una versión anterior del controlador siguiendo alguno de los siguientes métodos:
	
	• Instale la versión anterior
	
	1. Descargue el paquete de la versión anterior desde el enlace que aparece en esta tabla (versión 2.2.3).
	2. Ejecute el script de instalación de PowerShell install.ps1.
	
	Para obtener más información sobre los pasos previos y posteriores a la instalación, consulte Habilitar redes mejoradas en Windows.
	
	Utilice Amazon EC2 Systems Manager para una actualización masiva
	
	• Realice una actualización masiva a través del documento `AWS-ConfigureAWSPackage` de SSM, con los siguientes parámetros:
	  • Nombre: AwsEnaNetworkDriver
	  • Versión: 2.2.3
		26 de octubre de 2021

Versión de controlador	Detalles	Fecha de la versión
2.2.3	Nueva característica • Añade soporte para nuevas tarjetas Nitro con redes de instancias de hasta 400 Gbps. Corrección de errores • Corrige la condición de carrera entre el cambio de tiempo del sistema y la consulta de tiempo del sistema por parte del controlador de ENA, lo que provoca la detección falsa positiva de la falta de respuesta del hardware. La versión 2.2.3 del controlador Windows ENA es la versión final compatible con Windows Server 2008 R2. Los tipos de instancias disponibles actualmente que utilizan ENA seguirán siendo compatibles con Windows Server 2008 R2 y los controladores están disponibles mediante descarga. Ningún tipo de instancias futuras será compatible con Windows Server 2008 R2 y no podrá iniciar, importar ni migrar imágenes de Windows Server 2008 R2 a futuros tipos de instancias.	25 de marzo de 2021

Versión de controlador	Detalles	Fecha de la versión
2.2.2	Nueva característica • Agregue soporte para consultar métricas de rendimiento del adaptador de red con CloudWatch y los contadores de rendimiento para consumidores de Windows. Corrección de errores • Soluciona problemas de rendimiento en instancias bare metal.	21 de diciembre de 2020
2.2.1	Nueva característica • Agrega un método para permitir que el host consulte el adaptador de red elástico para obtener métricas de rendimiento de red.	1 de octubre de 2020

Versión de controlador	Detalles	Fecha de la versión
2.2.0	Nuevas características • Da soporte a los tipos de hardware de próxima generación. • Mejora el tiempo de inicio de las instancias después de reanudar la parada de hibernación y elimina los mensajes de error de ENA que sean falsos positivos. Optimizaciones de rendimiento • Optimiza el procesamiento del tráfico entrante. • Mejora la administración de memoria compartida en entornos de recursos bajos. Corrección de errores • Evita el bloqueo del sistema tras la eliminación del dispositivo ENA en un escenario raro en el que el controlador no se puede restablecer.	12 de agosto de 2020
2.1.5	Corrección de errores • Corrige errores ocasionales de inicialización del adaptador de red en instancias bare metal.	23 de junio de 2020

Versión de controlador	Detalles	Fecha de la versión
2.1.4	Correcciones de errores • Evita problemas de conectividad causados por metadatos de paquetes LSO corruptos que llegan de la pila de la red. • Impedir el bloqueo del sistema causado por una condición extraña que deriva en un acceso a una memoria de paquete ya liberada.	25 de noviembre de 2019
2.1.2	Nueva característica • Se agregó soporte para el informe de identificación del proveedor para permitir que el sistema operativo genere UUIDs basados en MAC. Correcciones de errores • Se ha mejorado el rendimiento de configuración de red DHCP durante la inicialización. • Calcule correctamente la suma de comprobación de L4 en el tráfico IPv6 entrante cuando la unidad de transmisión máxima (MTU) supere 4K. • Mejoras generales en la estabilidad del controlador y correcciones de errores menores.	4 de noviembre de 2019

Versión de controlador	Detalles	Fecha de la versión
2.1.1	Correcciones de errores • Evita caídas de paquetes TCP LSO muy fragmentados lleguen desde el sistema operativo. • Administre correctamente el protocolo Encapsulating Security Payload (ESP) dentro de IPSec en redes IPv6.	16 de septiembre de 2019

Versión de controlador	Detalles	Fecha de la versión

2.1.0	El controlador de ENA Windows v2.1 introduce nuevas capacidades de dispositivos ENA, proporciona un aumento del rendimiento, añade nuevas características e incluye varias mejoras de estabilidad.
	• Nuevas características
	  • Utilice la clave de registro estandarizada de Windows para configuración de tramas gigantes.
	  • Realice la configuración del ID de VLAN a través de la GUI de propiedades del controlador de ENA.
	  • Flujos de recuperación mejorados
	  • Mecanismo de identificación de fallos mejorado.
	  • Soporte añadido para parámetros de recuperación ajustable.
	  • Soporte de hasta 32 colas de E/S para instancias de EC2 más nuevas que tienen más de 8 vCPU.
	  • ~90 % de reducción de tamaño de memoria de controladores.
	• Optimizaciones de rendimiento
	  • Latencia de ruta de transmisión reducida.
	  • Soporte de descarga de suma de comprobación de recepción.
	  •
		1 de julio de 2019

Versión de controlador	Detalles	Fecha de la versión
	Optimización de rendimiento de sistema con carga elevada (uso optimizado de mecanismos de bloqueo). • Mejoras adicionales para reducir la utilización de CPU y mejorar la respuesta del sistema con carga. • Correcciones de errores • Corrección de fallo debido a un análisis no válido de encabezados Tx no contiguos. • Corrige los fallos del controlador v1.5 durante la desconexión de la interfaz de red elástica en instancias bare metal. • Corrección del error de cálculo de suma de comprobación de pseudoencabezado de LSO en IPv6. • Corrección de posible fuga de recursos de memoria tras un fallo de inicialización. • Deshabilitación de descarga de suma de comprobac ión de TCP/UDP para fragmentos de IPv4. • Corrección de configuración de VLAN. La VLAN se desactivaba incorrectamente cuando solo se debería haber deshabilitado la prioridad de VLAN. • Habilitación del análisis correcto de mensajes personalizados del controlador por el visor de eventos. •	

Versión de controlador	Detalles	Fecha de la versión
	Corrección de fallo para inicializar el controlador debido a una control de marca temporal incorrecto. • Corrección de la condición de carrera entre el procesamiento de datos y la deshabilitación del dispositivo ENA.	
1.5.0	• Mejoras de la estabilidad y correcciones de rendimien to. • Ahora los búferes de recepción se pueden configura r con un valor de hasta 8192 en las Propiedades avanzadas del NIC de ENA. • El valor predeterminado es de 1k.	4 de octubre de 2018
1.2.3	Incluye correcciones de fiabilidad y unifica el soporte para Windows Server 2008 R2 hasta Windows Server 2016.	13 de febrero de 2018
1.0.8	La versión inicial. Se incluye en las AMI para Windows Server 2008 R2, Windows Server 2012 RTM, Windows Server 2012 R2 y Windows Server 2016.	de julio de 2016

Amazon SNS puede notificarle cuando se publiquen nuevas versiones de los controladores de Windows para EC2. Para suscribirse a estas notificaciones, utilice el siguiente procedimiento.

Para suscribirse a las notificaciones de EC2

1. Abra la consola de Amazon SNS en https://console.aws.amazon.com/sns/v3/home.
2. En la barra de navegación, cambie la región a EE. UU. Este (Norte de Virginia), si es necesario. Debe seleccionar esta región porque las notificaciones de SNS a las que se va a suscribir están en esa región.

3. En el panel de navegación, seleccione Subscriptions.
4. Seleccione Create subscription.
5. En el cuadro de diálogo Crear suscripción, haga lo siguiente:
   a. En ARN de tema, copie el siguiente nombre de recurso de Amazon (ARN):

      arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers
   b. En Protocolo, elija `Email`.
   c. En Punto de conexión, escriba una dirección de correo electrónico que pueda utilizar para recibir notificaciones.
   d. Seleccione Crear subscripción.
6. Debe recibir un correo electrónico de confirmación. Abra el mensaje y siga las instrucciones para completar la suscripción.

Cuando se publican nuevos controladores de Windows para EC2, enviamos notificaciones a los suscriptores. Si ya no desea recibir estas notificaciones, utilice el siguiente procedimiento para cancelar la suscripción.

Para anular la suscripción a las notificaciones del controlador de Windows para Amazon EC2

1. Abra la consola de Amazon SNS en https://console.aws.amazon.com/sns/v3/home.
2. En el panel de navegación, seleccione Subscriptions.
3. Seleccione la casilla de verificación de la suscripción y, a continuación, elija Acciones, Eliminar suscripciones. Cuando se le pida confirmación, seleccione Eliminar.

Mejora del rendimiento de la red con ENA Express en las instancias EC2

ENA Express funciona con la tecnología Scalable Reliable Datagram (SRD) de AWS. SRD es un protocolo de transporte de red de alto rendimiento que utiliza el enrutamiento dinámico para aumentar el rendimiento y minimizar la latencia de cola. Con ENA Express, puede establecer comunicación entre dos instancias de EC2 en la misma zona de disponibilidad.

Ventajas de ENA Express

- Aumenta el ancho de banda máximo que puede utilizar un único flujo de 5 Gbps a 25 Gbps en la subred, hasta el límite de instancias agregado.

- Reduce la latencia final del tráfico de red entre instancias de EC2, especialmente durante periodos de alta carga de red.
- Detecta y evita las rutas de red sobrecargadas.
- Gestiona algunas tareas directamente en la capa de red, como la reordenación de paquetes en el extremo receptor y la mayoría de las retransmisiones necesarias. Esto libera la capa de aplicación para otras tareas.

> **Note**
>
> Si su aplicación envía o recibe un gran volumen de paquetes por segundo y necesita optimizar la latencia la mayor parte del tiempo, especialmente durante los períodos en los que no hay congestión en la red, Redes mejoradas podría ser una mejor opción para su red.

Durante los periodos en los que el tráfico de red sea bajo, es posible que observe un ligero aumento en la latencia de los paquetes (decenas de microsegundos) cuando el paquete utilice ENA Express. Durante esos momentos, las aplicaciones que priorizan características específicas de rendimiento de la red pueden beneficiarse de ENA Express de la siguiente manera:

- Los procesos pueden beneficiarse del aumento del ancho de banda máximo de flujo único de 5 Gbps a 25 Gbps dentro de la misma zona de disponibilidad, hasta el límite de instancias agregado. Por ejemplo, si un tipo de instancia específico admite hasta 12,5 Gbps, el ancho de banda de flujo único también está limitado a 12,5 Gbps.
- Los procesos que se ejecutan durante más tiempo deberían experimentar una latencia de cola reducida durante los períodos de congestión de la red.
- Los procesos pueden beneficiarse de una distribución más uniforme y estándar de los tiempos de respuesta de la red.

Requisitos previos para instancias de Linux

Para asegurarse de que ENA Express puede funcionar eficazmente, actualice la configuración de la instancia de la siguiente manera.

- Si la instancia usa marcos gigantes, ejecute el siguiente comando para establecer su unidad de transmisión máxima (MTU) en `8900`.

```
[ec2-user ~]$ sudo ip link set dev eth0 mtu 8900
```

- Aumente el tamaño del anillo del receptor (Rx), como se indica a continuación:

```
[ec2-user ~]$ ethtool -G device rx 8192
```

- Para maximizar el ancho de banda de ENA Express, configure los límites de cola de TCP de la siguiente manera:

  1. Establezca el límite de colas pequeñas de TCP en 1 MB o más. Esto aumenta la cantidad de datos que están en cola para su transmisión en un socket.

     ```
     sudo sh -c 'echo 1048576 > /proc/sys/net/ipv4/tcp_limit_output_bytes'
     ```

  2. Deshabilite los límites de cola de bytes en el dispositivo eth si están habilitados para su distribución de Linux. Esto aumenta los datos en cola que se van a transmitir en la cola del dispositivo.

     ```
     sudo sh -c 'for txq in /sys/class/net/eth0/queues/tx-*; do echo max > ${txq}/
     byte_queue_limits/limit_min; done'
     ```

     > **Note**
     >
     > El controlador ENA de la distribución de Amazon Linux desactiva los límites de cola de bytes de forma predeterminada.

Cómo funciona ENA Express

ENA Express funciona con la tecnología Scalable Reliable Datagram (SRD) de AWS. Distribuye los paquetes para cada flujo de red a través de diferentes rutas de red de AWS y ajusta dinámicamente la distribución cuando detecta indicios de congestión. También gestiona la reordenación de paquetes en el extremo receptor.

Para garantizar que ENA Express pueda gestionar el tráfico de red según lo previsto, las instancias emisoras y receptoras, y la comunicación entre dichas instancias deben cumplir todos los requisitos siguientes:

- Se admiten los tipos de instancia de envío y recepción. Para obtener más información, consulte la tabla Tipos de instancia compatibles con ENA Express.
- Tanto las instancias de envío como las de recepción deben tener configurado ENA Express. Si hay diferencias en la configuración, puede encontrarse con situaciones en las que el tráfico adopte por defecto la transmisión ENA estándar. El siguiente escenario muestra lo que puede ocurrir.

  Escenario: diferencias en la configuración

instancia	ENA Express habilitado	UDP usa ENA Express
instancia 1	Sí	Sí
instancia 2	Sí	No

  En este caso, el tráfico TCP entre las dos instancias puede utilizar ENA Express, ya que ambas instancias lo habilitaron. Sin embargo, dado que una de las instancias no utiliza ENA Express para el tráfico de UDP, la comunicación entre estas dos instancias a través de UDP utiliza la transmisión ENA estándar.
- Las instancias de envío y recepción deben ejecutarse en la misma zona de disponibilidad.
- La ruta de red entre las instancias no debe incluir cajas de middleware. ENA Express no admite actualmente cajas de middleware.
- (Solo instancias de Linux) Para aprovechar todo el potencial del ancho de banda, utilice la versión 2.2.9 o superior del controlador.
- (Solo instancias de Linux) Para generar métricas, utilice la versión 2.8 o superior del controlador.

Si no se cumple algún requisito, las instancias utilizan el protocolo TCP/UDP estándar, pero sin SRD para comunicarse.

Para asegurarse de que el controlador de red de su instancia está configurado para un rendimiento óptimo, revise las prácticas recomendadas para los controladores ENA. Estas prácticas recomendadas también se aplican a ENA Express. Para obtener más información, consulte Guía sobre la optimización de rendimiento y las prácticas recomendadas para el controlador ENA de Linux en el sitio web de GitHub.

> **Note**
>
> Amazon EC2 se refiere a la relación entre una instancia y una interfaz de red conectada a ella como un adjunto. La configuración de ENA Express se aplica al adjunto. Si la interfaz de red se desvincula de la instancia, el adjunto deja de existir y la configuración de ENA Express que se le aplicaba deja de estar vigente. Lo mismo ocurre cuando se finaliza una instancia, aunque la interfaz de red permanezca.

Tipos de instancia compatibles con ENA Express

Las siguientes pestañas contienen los tipos de instancias compatibles con ENA Express.

General purpose

Tipo de instancia	Arquitectura
m6a.12xlarge	x86_64
m6a.16xlarge	x86_64
m6a.24xlarge	x86_64
m6a.32xlarge	x86_64
m6a.48xlarge	x86_64
m6a.metal	x86_64
m6i.8xlarge	x86_64
m6i.12xlarge	x86_64
m6i.16xlarge	x86_64
m6i.24xlarge	x86_64
m6i.32xlarge	x86_64
m6i.metal	x86_64

Tipo de instancia	Arquitectura
m6id.8xlarge	x86_64
m6id.12xlarge	x86_64
m6id.16xlarge	x86_64
m6id.24xlarge	x86_64
m6id.32xlarge	x86_64
m6id.metal	x86_64
m7g.12xlarge	arm64
m7g.16xlarge	arm64
m7g.metal	arm64
m7gd.12xlarge	arm64
m7gd.16xlarge	arm64
m7gd.metal	arm64
m7i.12xlarge	x86_64
m7i.16xlarge	x86_64
m7i.24xlarge	x86_64
m7i.48xlarge	x86_64
m7i.metal-24xl	x86_64
m7i.metal-48xl	x86_64

Compute optimized

Tipo de instancia	Arquitectura
c6a.12xlarge	x86_64
c6a.16xlarge	x86_64
c6a.24xlarge	x86_64
c6a.32xlarge	x86_64
c6a.48xlarge	x86_64
c6a.metal	x86_64
c6gn.16xlarge	arm64
c6i.8xlarge	x86_64
c6i.12xlarge	x86_64
c6i.16xlarge	x86_64
c6i.24xlarge	x86_64
c6i.32xlarge	x86_64
c6i.metal	x86_64
c6id.8xlarge	x86_64
c6id.12xlarge	x86_64
c6id.16xlarge	x86_64
c6id.24xlarge	x86_64
c6id.32xlarge	x86_64
c6id.metal	x86_64

Tipo de instancia	Arquitectura
c7g.12xlarge	arm64
c7g.16xlarge	arm64
c7g.metal	arm64
c7gd.12xlarge	arm64
c7gd.16xlarge	arm64
c7gd.metal	arm64
c7i.12xlarge	x86_64
c7i.16xlarge	x86_64
c7i.24xlarge	x86_64
c7i.48xlarge	x86_64
c7i.metal-24xl	x86_64
c7i.metal-48xl	x86_64

Memory optimized

Tipo de instancia	Arquitectura
r6a.12xlarge	x86_64
r6a.16xlarge	x86_64
r6a.24xlarge	x86_64
r6a.32xlarge	x86_64
r6a.48xlarge	x86_64

Tipo de instancia	Arquitectura
r6a.metal	x86_64
r6i.8xlarge	x86_64
r6i.12xlarge	x86_64
r6i.16xlarge	x86_64
r6i.24xlarge	x86_64
r6i.32xlarge	x86_64
r6i.metal	x86_64
r6id.8xlarge	x86_64
r6id.12xlarge	x86_64
r6id.16xlarge	x86_64
r6id.24xlarge	x86_64
r6id.32xlarge	x86_64
r6id.metal	x86_64
r7g.12xlarge	arm64
r7g.16xlarge	arm64
r7g.metal	arm64
r7gd.12xlarge	arm64
r7gd.16xlarge	arm64
r7gd.metal	arm64
r7i.12xlarge	x86_64

Tipo de instancia	Arquitectura
r7i.16xlarge	x86_64
r7i.24xlarge	x86_64
r7i.48xlarge	x86_64
r7i.metal-24xl	x86_64
r7i.metal-48xl	x86_64
u7i-12tb.224xlarge	x86_64
u7in-16tb.224xlarge	x86_64
u7in-24tb.224xlarge	x86_64
u7in-32tb.224xlarge	x86_64
x2idn.16xlarge	x86_64
x2idn.24xlarge	x86_64
x2idn.32xlarge	x86_64
x2idn.metal	x86_64
x2iedn.8xlarge	x86_64
x2iedn.16xlarge	x86_64
x2iedn.24xlarge	x86_64
x2iedn.32xlarge	x86_64
x2iedn.metal	x86_64

Accelerated computing

Tipo de instancia	Arquitectura
g6.48xlarge	x86_64

Storage optimized

Tipo de instancia	Arquitectura
i4g.4xlarge	arm64
i4g.8xlarge	arm64
i4g.16xlarge	arm64
i4i.8xlarge	x86_64
i4i.12xlarge	x86_64
i4i.16xlarge	x86_64
i4i.24xlarge	x86_64
i4i.32xlarge	x86_64
i4i.metal	x86_64
im4gn.4xlarge	arm64
im4gn.8xlarge	arm64
im4gn.16xlarge	arm64

Enumerar y ver la configuración de ENA Express

En esta sección, se explica cómo enumerar y ver la información de ENA Express desde la AWS Management Console o desde la AWS CLI. Para obtener más información, seleccione la pestaña correspondiente al método que vaya a utilizar.

Console

En esta pestaña, se explica cómo encontrar información sobre la configuración actual de ENA Express y ver la compatibilidad con los tipos de instancia en la AWS Management Console.

Ver compatibilidad con los tipos de instancias

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación izquierdo, elija Tipos de instancias.
3. Seleccione un tipo de instancia para ver los detalles de esa instancia. Puede elegir el enlace Tipo de instancia para abrir la página de detalles o puede seleccionar la casilla de la parte izquierda de la lista para ver los detalles en el panel correspondiente, en la parte inferior de la página.
4. En la pestaña Redes o en esa sección de la página de detalles, Compatibilidad con ENA Express muestra un valor verdadero o falso para indicar si el tipo de instancia admite esta característica.

Ver la configuración de la lista de interfaces de red

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación izquierdo, elija Network Interfaces (Interfaces de red).
3. Seleccione una interfaz de red para ver los detalles de esa instancia. Puede elegir el enlace ID de interfaz de red para abrir la página de detalles o puede seleccionar la casilla de la parte izquierda de la lista para ver los detalles en el panel correspondiente, en la parte inferior de la página.
4. En la sección de Adjunto de la interfaz de red de la pestaña Detalles o la página de detalles, revise la configuración de ENA Express y UDP de ENA Express.

Ver la configuración de las instancias

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación izquierdo, elija instancias.
3. Seleccione una instancia para ver sus detalles. Puede elegir el enlace ID de instancia para abrir la página de detalles o puede seleccionar la casilla de la parte izquierda de la lista para ver los detalles en el panel correspondiente, en la parte inferior de la página.

4. En la sección Interfaces de red de la pestaña Redes, desplácese hacia la derecha para revisar la configuración de ENA Express y UDP de ENA Express.

AWS CLI

En esta pestaña, se explica cómo encontrar información sobre la configuración actual de ENA Express y ver la compatibilidad con los tipos de instancia en la AWS CLI.

Describir los tipos de instancias

Para obtener información sobre la configuración del tipo de instancia para un tipo de instancia específico, ejecute el comando describe-instance-types en la AWS CLI y sustituya el tipo de instancia como se indica a continuación:

```
[ec2-user ~]$ aws ec2 describe-instance-types --instance-types m6i.metal
{
"InstanceTypes": [
{
 "InstanceType": "m6i.metal",
 "CurrentGeneration": true,
 ...
 },
 "NetworkInfo": {
  ...
  "EnaSrdSupported": true
 },
 ...
}
]
}
```

Descripción de instancias

Para obtener información sobre la configuración de ENA Express para instancias específicas, ejecute el comando describe-instances en la AWS CLI como se indica a continuación: Este ejemplo de comando devuelve una lista de las configuraciones de ENA Express para las interfaces de red asociadas a cada una de las instancias en ejecución especificadas por el parámetro `--instance-ids`.

```
[ec2-user ~]$ aws ec2 describe-instances --instance-
ids i-1234567890abcdef0 i-0598c7d356eba48d7 --query 'Reservations[*].Instances[*].
[InstanceId, NetworkInterfaces[*].Attachment.EnaSrdSpecification]'[
 [
  [
   "i-1234567890abcdef0",
   [
    {
     "EnaSrdEnabled": true,
     "EnaSrdUdpSpecification": {
      "EnaSrdUdpEnabled": false
     }
    }
   ]
  ]
 ],
 [
  [
   "i-0598c7d356eba48d7",
   [
    {
     "EnaSrdEnabled": true,
     "EnaSrdUdpSpecification": {
      "EnaSrdUdpEnabled": false
     }
    }
   ]
  ]
 ]
]
```

Describir las interfaces de red

Para obtener información sobre la configuración de ENA Express para una interfaz de red, ejecute el comando describe-network-interfaces en la AWS CLI como se indica a continuación:

```
[ec2-user ~]$ aws ec2 describe-network-interfaces
{
"NetworkInterfaces": [
{
 "Association": {
  ....IPs, DNS...
 },
```

```
 "Attachment": {
  "AttachTime": "2022-11-17T09:04:28+00:00",
  "AttachmentId": "eni-attach-0ab1c23456d78e9f0",
  "DeleteOnTermination": true,
  "DeviceIndex": 0,
  "NetworkCardIndex": 0,
  "InstanceId": "i-1234567890abcdef0",
  "InstanceOwnerId": "111122223333",
  "Status": "attached",
  "EnaSrdSpecification": {
   "EnaSrdEnabled": true,
   "EnaSrdUdpSpecification": {
    "EnaSrdUdpEnabled": true
   }
  }
 },
 ...
 "NetworkInterfaceId": "eni-1234567890abcdef0",
 "OwnerId": "111122223333",
 ...
}
]
}
```

PowerShell

En esta pestaña, se explica cómo encontrar información sobre la configuración actual de ENA Express y ver la compatibilidad con los tipos de instancia con PowerShell.

Describir los tipos de instancias

Para obtener información sobre la configuración del tipo de instancia para un tipo de instancia específico, ejecute Get-EC2InstanceType Cmdlet en las herramientas para PowerShell y sustituya el tipo de instancia como se indica a continuación:

```
PS C:\> Get-EC2InstanceType -InstanceType m6i.metal | `
Select-Object `
    InstanceType,
    CurrentGeneration,
    @{Name = 'EnaSrdSupported'; Expression = { $_.NetworkInfo.EnaSrdSupported } } |
 `
Format-List
```

```
InstanceType      : m6i.metal
CurrentGeneration : True
EnaSrdSupported   : True
```

Si ENA Express está activada, se devuelve un valor de `True`.

Describir las interfaces de red

Para obtener información sobre la configuración de ENA Express para una interfaz de red, ejecute Get-EC2NetworkInterface Cmdlet con las herramientas para PowerShell de la siguiente manera:

```
PS C:\> Get-EC2NetworkInterface -NetworkInterfaceId eni-0d1234e5f6a78901b | `
Select-Object `
    Association,
    NetworkInterfaceId,
    OwnerId,
    @{Name = 'AttachTime'; Expression = { $_.Attachment.AttachTime } },
    @{Name = 'AttachmentId'; Expression = { $_.Attachment.AttachmentId } },
    @{Name = 'DeleteOnTermination'; Expression =
 { $_.Attachment.DeleteOnTermination } },
    @{Name = 'NetworkCardIndex'; Expression = { $_.Attachment.NetworkCardIndex } },
    @{Name = 'InstanceId'; Expression = { $_.Attachment.InstanceId } },
    @{Name = 'InstanceOwnerId'; Expression = { $_.Attachment.InstanceOwnerId } },
    @{Name = 'Status'; Expression = { $_.Attachment.Status } },
    @{Name = 'EnaSrdEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdEnabled } },
    @{Name = 'EnaSrdUdpEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdUdpSpecification.EnaSrdUdpEnabled } }

Association         :
NetworkInterfaceId  : eni-0d1234e5f6a78901b
OwnerId             : 111122223333
AttachTime          : 6/11/2022 1:13:11 AM
AttachmentId        : eni-attach-0d1234e5f6a78901b
DeleteOnTermination : True
NetworkCardIndex    : 0
InstanceId          : i-0d1234e5f6a78901b
InstanceOwnerId     : 111122223333
Status              : attached
EnaSrdEnabled       : True
EnaSrdUdpEnabled    : False
```

Configurar ENA Express

Puede configurar ENA Express para los tipos de instancia de EC2 compatibles sin necesidad de instalar ningún software adicional.

En esta sección, se explica cómo configurar ENA Express desde la AWS Management Console o desde la AWS CLI. Para obtener más información, seleccione la pestaña correspondiente al método que vaya a utilizar.

Console

En esta pestaña se explica cómo administrar la configuración de ENA Express para las interfaces de red adjuntas a una instancia.

Administrar ENA Express desde la lista de interfaces de red

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación izquierdo, elija Network Interfaces (Interfaces de red).
3. Seleccione una interfaz de red que esté adjunta a una instancia. Puede elegir el enlace ID de interfaz de red para abrir la página de detalles o puede seleccionar la casilla de la parte izquierda de la lista.
4. Elija Administrar ENA Express en el menú Acción de la parte superior derecha de la página. Se abre el cuadro de diálogo Administrar ENA Express, en el que se muestran el ID de la interfaz de red seleccionada y la configuración actual.

> **Note**
>
> Si la interfaz de red que seleccionó no está adjunta a una instancia, esta acción no aparece en el menú.

5. Para usar ENA Express, seleccione la casilla Habilitar.
6. Cuando ENA Express está habilitado, puede configurar los ajustes de UDP. Para usar UDP de ENA Express, seleccione la casilla Habilitar.
7. Elija Guardar para guardar las opciones de configuración.

Administrar ENA Express desde la lista de instancias

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

2. En el panel de navegación izquierdo, elija instancias.
3. Seleccione la instancia que desea administrar. Puede elegir el ID de instancia para abrir la página de detalles o puede seleccionar la casilla de la parte izquierda de la lista.
4. Seleccione la interfaz de red que desea configurar para su instancia.
5. Elija Manage ENA Express (Administrar ENA Express) en el menú Action (Acción) de la parte superior derecha de la página.
6. Para configurar ENA Express para una interfaz de red adjunta a la instancia, selecciónela en la lista Interfaz de red.
7. Para utilizar ENA Express para el adjunto de la interfaz de red seleccionado, seleccione la casilla Habilitar.
8. Cuando ENA Express está habilitado, puede configurar los ajustes de UDP. Para usar UDP de ENA Express, seleccione la casilla Habilitar.
9. Elija Save (Guardar) para guardar las opciones de configuración.

Configurar ENA Express al adjuntar una interfaz de red a una instancia de EC2

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación izquierdo, elija Network Interfaces (Interfaces de red).
3. Seleccione una interfaz de red que no esté adjunta a una instancia (el valor de Estado es Disponible). Puede elegir el enlace Network interface ID (ID de interfaz de red) para abrir la página de detalles o puede seleccionar la casilla de la parte izquierda de la lista.
4. Seleccione la instancia a la que se adjuntará.
5. Para usar ENA Express después de adjuntar la interfaz de red a la instancia, seleccione la casilla Habilitar.
6. Cuando ENA Express está habilitado, puede configurar los ajustes de UDP. Para usar UDP de ENA Express, seleccione la casilla Enable (Habilitar).
7. Para conectar la interfaz de red a la instancia y guardar la configuración de ENA Express, elija Adjuntar.

AWS CLI

Esta pestaña explica cómo configurar los ajustes de ENA Express en la AWS CLI.

Configurar ENA Express al adjuntar una interfaz de red

Para configurar ENA Express al adjuntar una interfaz de red a una instancia, ejecute el comando attach-network-interface en la AWS CLI, como se muestra en los siguientes ejemplos:

Ejemplo 1: usar ENA Express para el tráfico TCP, pero no para el tráfico UDP

En este ejemplo, configuramos `EnaSrdEnabled` como verdadero y permitimos que el valor predeterminado de `EnaSrdUdpEnabled` sea falso.

```
[ec2-user ~]$ aws ec2 attach-network-interface --network-interface-
id eni-0123f4567890a1b23 --instance-id i-0f1a234b5cd67e890 --device-index 1 --ena-
srd-specification 'EnaSrdEnabled=true'
{
"AttachmentId": "eni-attach-012c3d45e678f9012"
}
```

Ejemplo 2: usar ENA Express tanto para el tráfico TCP como para el tráfico UDP

En este ejemplo, `EnaSrdEnabled` y `EnaSrdUdpEnabled` se configuran como verdadero.

```
[ec2-user ~]$ aws ec2 attach-network-interface --network-interface-
id eni-0123f4567890a1b23 --instance-id i-0f1a234b5cd67e890 --device-index 1 --ena-
srd-specification
 'EnaSrdEnabled=true,EnaSrdUdpSpecification={EnaSrdUdpEnabled=true}'
{
"AttachmentId": "eni-attach-012c3d45e678f9012"
}
```

Actualizar la configuración de ENA Express para el adjunto de interfaz de red

Para actualizar la configuración de ENA Express de una interfaz de red adjunta a una instancia, ejecute el comando modify-network-interface-attribute en la AWS CLI, como se muestra en los siguientes ejemplos:

Ejemplo 1: usar ENA Express para el tráfico TCP, pero no para el tráfico UDP

En este ejemplo, configuramos `EnaSrdEnabled` como verdadero y permitimos que el valor predeterminado de `EnaSrdUdpEnabled` sea falso si no se ha configurado previamente.

```
[ec2-user ~]$ aws ec2 modify-network-interface-attribute --network-interface-
id eni-0123f4567890a1b23 --ena-srd-specification 'EnaSrdEnabled=true'
```

Ejemplo 2: usar ENA Express tanto para el tráfico TCP como para el tráfico UDP

En este ejemplo, `EnaSrdEnabled` y `EnaSrdUdpEnabled` se configuran como true (verdadero).

```
[ec2-user ~]$ aws ec2 modify-network-interface-attribute --
network-interface-id eni-0123f4567890a1b23 --ena-srd-specification
 'EnaSrdEnabled=true,EnaSrdUdpSpecification={EnaSrdUdpEnabled=true}'
```

Ejemplo 3: dejar de usar ENA Express para el tráfico UDP

En este ejemplo, `EnaSrdUdpEnabled` se configura como falso.

```
[ec2-user ~]$ aws ec2 modify-network-interface-attribute --
network-interface-id eni-0123f4567890a1b23 --ena-srd-specification
 'EnaSrdUdpSpecification={EnaSrdUdpEnabled=false}'
```

PowerShell

Esta pestaña explica cómo configurar los ajustes de ENA Express con PowerShell.

Configurar ENA Express al adjuntar una interfaz de red

Para configurar los ajustes de ENA Express para una interfaz de red, ejecute Add-EC2NetworkInterface Cmdlet con las herramientas para PowerShell de la siguiente manera:

Ejemplo 1: usar ENA Express para el tráfico TCP, pero no para el tráfico UDP

En este ejemplo, configuramos `EnaSrdEnabled` como verdadero y permitimos que el valor predeterminado de `EnaSrdUdpEnabled` sea falso.

```
PS C:\> Add-EC2NetworkInterface `
-NetworkInterfaceId eni-0123f4567890a1b23 `
-InstanceId i-0f1a234b5cd67e890 `
-DeviceIndex 1 `
-EnaSrdSpecification_EnaSrdEnabled $true

eni-attach-012c3d45e678f9012
```

Ejemplo 2: usar ENA Express tanto para el tráfico TCP como para el tráfico UDP

En este ejemplo, `EnaSrdEnabled` y `EnaSrdUdpEnabled` se configuran como verdadero.

```
PS C:\> Add-EC2NetworkInterface `
-NetworkInterfaceId eni-0123f4567890a1b23 `
-InstanceId i-0f1a234b5cd67e890 `
-DeviceIndex 1 `
-EnaSrdSpecification_EnaSrdEnabled $true `
-EnaSrdUdpSpecification_EnaSrdUdpEnabled $true

eni-attach-012c3d45e678f9012
```

Actualizar la configuración de ENA Express para el adjunto de interfaz de red

Para actualizar los ajustes de ENA Express de una interfaz de red adjunta a una instancia, ejecute el comando Add-EC2NetworkInterface Cmdlet en las herramientas para PowerShell, tal como se muestra en los siguientes ejemplos:

Ejemplo 1: usar ENA Express para el tráfico TCP, pero no para el tráfico UDP

En este ejemplo, configuramos `EnaSrdEnabled` como verdadero y permitimos que el valor predeterminado de `EnaSrdUdpEnabled` sea falso si no se ha configurado previamente.

```
PS C:\> Edit-EC2NetworkInterfaceAttribute `
-NetworkInterfaceId eni-0123f4567890a1b23 `
-EnaSrdSpecification_EnaSrdEnabled $true ;
Get-EC2NetworkInterface -NetworkInterfaceId eni-0123f4567890a1b23 | `
Select-Object `
    NetworkInterfaceId,
    @{Name = 'EnaSrdEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdEnabled }},
    @{Name = 'EnaSrdUdpEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdUdpSpecification.EnaSrdUdpEnabled }} | `
Format-List

NetworkInterfaceId : eni-0123f4567890a1b23
EnaSrdEnabled      : True
EnaSrdUdpEnabled   : False
```

Ejemplo 2: usar ENA Express tanto para el tráfico TCP como para el tráfico UDP

En este ejemplo, `EnaSrdEnabled` y `EnaSrdUdpEnabled` se configuran como true (verdadero).

```
PS C:\> Edit-EC2NetworkInterfaceAttribute `
-NetworkInterfaceId eni-0123f4567890a1b23 `
```

```
-EnaSrdSpecification_EnaSrdEnabled $true `
-EnaSrdSpecification_EnaSrdUdpSpecification_EnaSrdUdpEnabled $true ;
Get-EC2NetworkInterface -NetworkInterfaceId eni-0123f4567890a1b23 | `
Select-Object `
    NetworkInterfaceId,
    @{Name = 'EnaSrdEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdEnabled }},
    @{Name = 'EnaSrdUdpEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdUdpSpecification.EnaSrdUdpEnabled }} | `
Format-List

NetworkInterfaceId : eni-0123f4567890a1b23
EnaSrdEnabled      : True
EnaSrdUdpEnabled   : True
```

Ejemplo 3: dejar de usar ENA Express para el tráfico UDP

En este ejemplo, `EnaSrdUdpEnabled` se configura como falso.

```
PS C:\> Edit-EC2NetworkInterfaceAttribute `
-NetworkInterfaceId eni-0123f4567890a1b23 `
-EnaSrdSpecification_EnaSrdUdpSpecification_EnaSrdUdpEnabled $false ;
Get-EC2NetworkInterface -NetworkInterfaceId eni-0123f4567890a1b23 | `
Select-Object `
    NetworkInterfaceId,
    @{Name = 'EnaSrdEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdEnabled }},
    @{Name = 'EnaSrdUdpEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdUdpSpecification.EnaSrdUdpEnabled }} | `
Format-List

NetworkInterfaceId : eni-0123f4567890a1b23
EnaSrdEnabled      : True
EnaSrdUdpEnabled   : False
```

Configuración de ENA Express en la inicialización

Puede utilizar uno de los métodos siguientes para configurar ENA Express para una AMI cuando lance una instancia desde la AWS Management Console.

- Puede configurar ENA Express para su AMI al iniciar una instancia con el asistente de inicialización de instancias. Para obtener información sobre la configuración, consulte

Configuración de red avanzada en Network settings (Configuración de red) para el asistente de inicialización de instancias.

- Puede configurar ENA Express para su AMI cuando utilice una plantilla de inicialización. Para obtener más información sobre la configuración de la plantilla de inicialización, consulte Configuración de red avanzada en Network settings (Configuración de red) para plantillas de inicialización.

Supervisar el rendimiento de ENA Express

Después de habilitar ENA Express para los adjuntos de interfaz de red tanto en la instancia de envío como en la de recepción, puede utilizar las métricas de ENA Express para asegurarse de que sus instancias aprovechen al máximo las mejoras de rendimiento que proporciona la tecnología SRD.

Para ver una lista de las métricas que se filtran para ENA Express, ejecute el siguiente comando ethtool para su interfaz de red (que aquí se muestra como `eth0`):

```
[ec2-user ~]$ ethtool -S eth0 | grep ena_srd
NIC statistics:
 ena_srd_mode: 0
 ena_srd_tx_pkts: 0
 ena_srd_eligible_tx_pkts: 0
 ena_srd_rx_pkts: 0
 ena_srd_resource_utilization: 0
```

Verificar la configuración de ENA Express para una instancia

Para comprobar la configuración actual de ENA Express para el adjunto de la interfaz de red de la instancia, ejecute el comando `ethtool` para mostrar las métricas de ENA Express y tome nota del valor de la métrica `ena_srd_mode`. Los valores son los siguientes:

- `0` = ENA Express desactivado, UDP desactivado
- 1 = ENA Express activado, UDP desactivado
- 2 = ENA Express desactivado, UDP activado

> **Note**
>
> Esto solo ocurre cuando ENA Express se habilitó originalmente y UDP se configuró para usarlo. El valor anterior se retiene para el tráfico UDP.

- 3 = ENA Express activado, UDP activado

Después de habilitar ENA Express para el adjunto de interfaz de red en una instancia, la instancia de envío inicia la comunicación con la instancia de recepción y el SRD detecta si ENA Express funciona tanto en la instancia de envío como en la de recepción. Si ENA Express funciona, la comunicación puede utilizar la transmisión de SRD. Si ENA Express no funciona, la comunicación vuelve a la transmisión ENA estándar. Para confirmar si la transmisión de paquetes utiliza SRD, puede comparar el número de paquetes que cumplen los requisitos (métrica `ena_srd_eligible_tx_pkts`) con el número de paquetes SRD transmitidos (métrica `ena_srd_tx_pkts`) durante un periodo de tiempo determinado.

Puede supervisar el uso de recursos de SRD con la métrica `ena_srd_resource_utilization`. Si su instancia está a punto de agotar sus recursos de SRD, sabrá que llegó el momento de escalarla horizontalmente.

Para obtener más información sobre las métricas de ENA Express, consulte Métricas para ENA Express.

Configuración de ENA Express para optimizar el rendimiento

A fin de comprobar la configuración de la instancia de Linux para un rendimiento óptimo de ENA Express, puede ejecutar el siguiente script que está disponible en el repositorio de Amazon GitHub:

https://github.com/amzn/amzn-ec2-ena-utilities/blob/main/ena-express/check-ena-express-settings.sh

El script ejecuta una serie de pruebas y sugiere cambios de configuración, tanto recomendados como necesarios.

Habilitación de redes mejoradas con la interfaz de Intel 82599 VF en instancias EC2

Amazon EC2 proporciona funcionalidades de red mejoradas a través de la interfaz Intel 82599 VF, que usa un controlador `ixgbevf` de Intel.

Contenido

- Habilitar redes mejoradas en la instancia
- Solucionar problemas de conectividad

Requisitos

Para prepararse para las redes mejoradas con la interfaz Intel 82599 VF, configure su instancia de la siguiente manera:

- Seleccione de entre los siguientes tipos de instancia compatibles: C3, C4, D2, I2, M4 (menos `m4.16xlarge`) y R3.
- Asegúrese de que la instancia tenga conexión a Internet.
- Si tiene datos importantes en la instancia que desea conservar, debería realizar ahora una copia de seguridad de esos datos creando una AMI desde la instancia. La actualización del kernel y los módulos del kernel, además de habilitar el atributo `sriovNetSupport`, puede hacer que las instancias o sistemas operativos incompatibles sean inaccesibles. Si tiene una copia de seguridad reciente y esto ocurre, los datos se conservarán.
- Instancias de Linux: lance la instancia desde una AMI HVM utilizando la versión de kernel de Linux 2.6.32 o posterior. Las AMI HVM de Amazon Linux más recientes tienen instaladas los módulos necesarios para las redes mejoradas y tienen establecidos los atributos necesarios. Por lo tanto, si inicia una instancia que admite redes mejoradas con respaldo de Amazon EBS utilizando una AMI HVM de Amazon Linux actual, las redes mejoradas ya están habilitadas para la instancia.

  > **Warning**
  >
  > Las redes mejoradas solo se admiten para instancias HVM. Si habilita las redes mejoradas con una instancia PV, podrían ser inaccesibles. Si establece este atributo sin el módulo o la versión del módulo adecuada, la instancia también podría ser inaccesible.

- Instancias de Windows: lance la instancia desde una AMI HVM de 64 bits. No se pueden habilitar las redes mejoradas en Windows Server 2008. Las redes mejoradas ya están habilitadas para las AMI de Windows Server 2012 R2 o Windows Server 2016 y versiones posteriores. Windows Server 2012 R2 incluye el controlador Intel 1.0.15.3 y recomendamos actualizar ese controlador a la versión más reciente con la utilidad Pnputil.exe.
- Utilice AWS CloudShell en la AWS Management Console, o bien instale y configure la AWS CLI o las AWS Tools for Windows PowerShell en cualquier computadora que elija, preferentemente en su equipo de escritorio o portátil local. Para obtener más información, consulte Acceder a Amazon

EC2 o la Guía del usuario de AWS CloudShell. Las redes mejoradas no se pueden administrar desde la consola de Amazon EC2.

Cómo verificar que el controlador esté instalado

Verifique que el controlador está instalado en su instancia.

Controlador de la interfaz de red de Linux

Utilice el siguiente comando para verificar si el módulo se está utilizando en una interfaz en particular, sustituyendo el nombre de la interfaz que quiere comprobar. Si utiliza una sola interfaz (predeterminada), esta será `eth0`. Si el sistema operativo admite nombres de red predecibles, podría ser un nombre como `ens5`.

En el ejemplo siguiente, el módulo `ixgbevf` no está cargado, ya que el controlador indicado es `vif`.

```
[ec2-user ~]$ ethtool -i eth0
driver: vif
version:
firmware-version:
bus-info: vif-0
supports-statistics: yes
supports-test: no
supports-eeprom-access: no
supports-register-dump: no
supports-priv-flags: no
```

En este caso, el módulo `ixgbevf` está cargado. Esta instancia tiene las redes mejoradas configuradas correctamente.

```
[ec2-user ~]$ ethtool -i eth0
driver: ixgbevf
version: 4.0.3
firmware-version: N/A
bus-info: 0000:00:03.0
supports-statistics: yes
supports-test: yes
supports-eeprom-access: no
supports-register-dump: yes
supports-priv-flags: no
```

Adaptador de red de Windows

Para comprobar si el controlador está instalado, conéctese a la instancia y abra Device Manager. Debería ver "Intel(R) 82599 Virtual Function" en la lista, en Adaptadores de red.

Probar si las redes mejoradas están habilitadas

Compruebe que el atributo `sriovNetSupport` esté configurado.

Atributo de instancia (sriovNetSupport)

Para comprobar si una instancia tiene establecido el atributo `sriovNetSupport` de las redes mejoradas, utilice uno de los siguientes comandos. Si se configuró el atributo, el valor es `simple`.

- describe-instance-attribute (AWS CLI) (AWS CLI/AWS CloudShell)

```
aws ec2 describe-instance-attribute --instance-id instance_id --attribute
 sriovNetSupport
```

- Get-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

```
Get-EC2InstanceAttribute -InstanceId instance-id -Attribute sriovNetSupport
```

Atributo de imagen (sriovNetSupport)

Para comprobar si una AMI ya tiene establecido el atributo `sriovNetSupport` de las redes mejoradas, utilice uno de los siguientes comandos. Si se configuró el atributo, el valor es `simple`.

- describe-images (AWS CLI)

```
aws ec2 describe-images --image-id ami_id --query "Images[].SriovNetSupport"
```

- Get-EC2Image (AWS Tools for Windows PowerShell)

```
(Get-EC2Image -ImageId ami-id).SriovNetSupport
```

Habilitar redes mejoradas en la instancia

El procedimiento que utiliza depende del sistema operativo de la instancia.

> **Warning**
>
> No hay ninguna forma de deshabilitar el atributo de redes mejoradas después de habilitarlo.

Amazon Linux

Las AMI HVM de Amazon Linux más recientes tienen instalado el módulo `ixgbevf` necesario para las redes mejoradas y tienen establecido el atributo `sriovNetSupport` que se necesita. Por lo tanto, si inicia un tipo de instancia utilizando una AMI HVM de Amazon Linux actual, las redes mejoradas ya están habilitadas para la instancia. Para obtener más información, consulte Probar si las redes mejoradas están habilitadas.

Si ha iniciado la instancia utilizando una AMI de Amazon Linux más antigua y no tiene habilitadas aún las redes mejoradas, utilice el siguiente procedimiento para habilitarlas.

Para habilitar las redes mejoradas

1. Conecte con la instancia .
2. Desde la instancia, ejecute el siguiente comando para actualizarla con el kernel y los módulos de kernel más recientes, incluido `ixgbevf`:

   ```
   [ec2-user ~]$ sudo yum update
   ```

3. Desde su equipo local, reinicie la instancia mediante la consola de Amazon EC2 o uno de los siguientes comandos: reboot-instances (AWS CLI), Restart-EC2Instance (AWS Tools for Windows PowerShell).
4. Conéctese de nuevo a la instancia y compruebe si el módulo `ixgbevf` está instalado y si tiene la versión mínima recomendada utilizando el comando modinfo ixgbevf de Probar si las redes mejoradas están habilitadas.
5. [instancia basada en EBS] Desde su equipo local, detenga la instancia mediante la consola de Amazon EC2 o uno de los siguientes comandos: stop-instances (AWS CLI), Stop-EC2Instance (AWS Tools for Windows PowerShell). Si la instancia la administra AWS OpsWorks, debe detenerla en la consola de AWS OpsWorks para mantener su estado sincronizado.

   [Instancia respaldada por el almacén de instancias] No puede detener la instancia para modificar el atributo. En lugar de ello, vaya a este procedimiento: Para habilitar las redes mejoradas (instancias con respaldo en el almacén de instancias).

6. En el equipo local, habilite el atributo de redes mejoradas con uno de los siguientes comandos:

   AWS CLI

   modify-instance-attribute (AWS CLI)

   ```
   aws ec2 modify-instance-attribute --instance-id instance_id --sriov-net-support
    simple
   ```

   PowerShell

   Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

   ```
   Edit-EC2InstanceAttribute -InstanceId instance_id -SriovNetSupport "simple"
   ```

7. (Opcional) Cree una AMI desde la instancia, tal y como se explica en Creación de una AMI basada en Amazon EBS. La AMI hereda el atributo de redes mejoradas de la instancia. Por lo tanto, puede utilizar esta AMI para iniciar otra instancia con las redes mejoradas habilitadas de manera predeterminada.
8. Desde su equipo local, inicie la instancia mediante la consola de Amazon EC2 o uno de los siguientes comandos: start-instances (AWS CLI), Start-EC2Instance (AWS Tools for Windows PowerShell). Si la instancia la administra AWS OpsWorks, debe iniciarla en la consola de AWS OpsWorks para mantener su estado sincronizado.
9. Conéctese a la instancia y compruebe que el módulo `ixgbevf` está instalado y cargado en la interfaz de red utilizando el comando ethtool -i eth***n*** command de Probar si las redes mejoradas están habilitadas.

Para habilitar las redes mejoradas (instancias con respaldo en el almacén de instancias)

Siga el procedimiento anterior hasta el paso en el que detiene la instancia. Cree una nueva AMI tal como se describe en Crear una AMI de Linux con respaldo en el almacén de instancias, asegurándose de habilitar el atributo de redes mejoradas cuando registre la AMI.

AWS CLI

register-image (AWS CLI/AWS CloudShell)

```
aws ec2 register-image --sriov-net-support simple ...
```

PowerShell

Register-EC2Image (AWS Tools for Windows PowerShell)

```
Register-EC2Image -SriovNetSupport "simple" ...
```

Ubuntu

Antes de comenzar, compruebe si las redes mejoradas ya están habilitadas en la instancia.

Las AMI HVM de Ubuntu de inicio rápido incluyen los controladores necesarios para las redes mejoradas. Si tiene una versión de `ixgbevf` anterior a 2.16.4, puede instalar el paquete del kernel de `linux-aws` para obtener los controladores de redes mejoradas más recientes.

En el siguiente procedimiento, se proporcionan los pasos generales para compilar el módulo `ixgbevf` en una instancia de Ubuntu.

Para instalar el paquete de kernel de **`linux-aws`**

1. Conéctese a la instancia.
2. Actualice la caché del paquete y los paquetes.

```
ubuntu:~$ sudo apt-get update && sudo apt-get upgrade -y linux-aws
```

> **Important**
>
> Si, durante el proceso de actualización, se le pide que instale `grub`, use `/dev/xvda` para instalar `grub` y luego elija conservar la versión actual de `/boot/grub/menu.lst`.

Otras distribuciones de Linux

Antes de comenzar, compruebe si las redes mejoradas ya están habilitadas en la instancia. Las últimas versiones de las AMI HVM de Ubuntu de inicio rápido incluyen los controladores necesarios para las redes mejoradas, por lo que no es necesario realizar pasos adicionales.

En el siguiente procedimiento, se proporcionan los pasos generales que debe realizar para habilitar las redes mejoradas con la interfaz Intel 82599 VF en una distribución de Linux que no sea Amazon

Linux o Ubuntu. Para obtener más información, como la sintaxis detallada de los comandos, las ubicaciones de los archivos o el soporte de paquetes y herramientas, consulte la documentación específica de su distribución de Linux.

Para habilitar las redes mejoradas en Linux

1. Conéctese a la instancia.
2. Descargue el código fuente para el módulo `ixgbevf` de su instancia desde Sourceforge en https://sourceforge.net/projects/e1000/files/ixgbevf%20stable/.

   Las versiones de `ixgbevf` anteriores a la 2.16.4, incluida la versión 2.14.2, no se compilan correctamente en algunas distribuciones de Linux, incluidas determinadas versiones de Ubuntu.
3. Compile e instale el módulo `ixgbevf` en la instancia.

   > **Warning**
   >
   > Si compila el módulo `ixgbevf` para el kernel actual y luego lo actualiza sin volver a compilar el controlador del nuevo kernel, es posible que el sistema vuelva al módulo `ixgbevf` específico de la distribución en el siguiente rearranque. Esto podría hacer que el sistema fuera inaccesible si la versión específica de la distribución es incompatible con las redes mejoradas.
4. Ejecute el comando sudo depmod para actualizar las dependencias de módulos.
5. Actualice `initramfs` en la instancia para asegurarse de que el nuevo módulo se carga en el momento del arranque.
6. Determine si el sistema utiliza de manera predeterminada nombres de interfaz de red predecibles. Los sistemas que utilizan las versiones 197 o posteriores de systemd o udev pueden cambiar el nombre de los dispositivos Ethernet y no garantizan que haya una sola interfaz de red denominada `eth0`. Este comportamiento puede producir problemas al conectarse a la instancia. Para obtener más información y para ver otras opciones de configuración, consulte Predictable Network Interface Names en el sitio web de freedesktop.org.

   a. Puede utilizar el siguiente comando para comprobar las versiones de systemd o udev en los sistemas basados en RPM:

   ```
   [ec2-user ~]$ rpm -qa | grep -e '^systemd-[0-9]\+\|^udev-[0-9]\+'
   systemd-208-11.el7_0.2.x86_64
   ```

En el ejemplo anterior de Red Hat Enterprise Linux 7, la versión de systemd es la 208, por lo que se deben deshabilitar los nombres de interfaz de red predecibles.

b. Para deshabilitar los nombres de interfaz de red predecibles, añada la opción `net.ifnames=0` a la línea `GRUB_CMDLINE_LINUX` en `/etc/default/grub`.

```
[ec2-user ~]$ sudo sed -i '/^GRUB\_CMDLINE\_LINUX/s/\"$/\ net\.ifnames\=0\"/' /
etc/default/grub
```

c. Vuelva a compilar el archivo de configuración de Grub.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

7. [Instancia basada en EBS] Desde su equipo local, detenga la instancia mediante la consola de Amazon EC2 o uno de los siguientes comandos: stop-instances (AWS CLI/AWS CloudShell), Stop-EC2Instance (AWS Tools for Windows PowerShell). Si la instancia la administra AWS OpsWorks, debe detenerla en la consola de AWS OpsWorks para mantener su estado sincronizado.

   [Instancia respaldada por el almacén de instancias] No puede detener la instancia para modificar el atributo. En lugar de ello, vaya a este procedimiento: Para habilitar las redes mejoradas (instancias con respaldo en el almacén de instancias).

8. En el equipo local, habilite el atributo de redes mejoradas con uno de los siguientes comandos:

   AWS CLI

   modify-instance-attribute (AWS CLI/AWS CloudShell)

   ```
   aws ec2 modify-instance-attribute --instance-id instance_id --sriov-net-support
    simple
   ```

   PowerShell

   Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

   ```
   Edit-EC2InstanceAttribute -InstanceId instance_id -SriovNetSupport "simple"
   ```

9. (Opcional) Cree una AMI desde la instancia, tal y como se explica en Creación de una AMI basada en Amazon EBS. La AMI hereda el atributo de redes mejoradas de la instancia. Por lo

tanto, puede utilizar esta AMI para iniciar otra instancia con las redes mejoradas habilitadas de manera predeterminada.

Si el sistema operativo de la instancia contiene un archivo `/etc/udev/rules.d/70-persistent-net.rules`, debe eliminarlo antes de crear la AMI. Este archivo contiene la dirección MAC del adaptador Ethernet de la instancia original. Si otra instancia arranca con este archivo, el sistema operativo no será capaz de encontrar el dispositivo y `eth0` producirá un error, lo que causará problemas de arranque. Este archivo se regenera en el siguiente ciclo de arranque y todas las instancias que se inician desde la AMI crean su propia versión del archivo.

10. Desde su equipo local, inicie la instancia mediante la consola de Amazon EC2 o uno de los siguientes comandos: start-instances (AWS CLI), Start-EC2Instance (AWS Tools for Windows PowerShell). Si la instancia la administra AWS OpsWorks, debe iniciarla en la consola de AWS OpsWorks para mantener su estado sincronizado.
11. (Opcional) Conéctese a la instancia y compruebe si el módulo está instalado.

Para habilitar las redes mejoradas (instancias con respaldo en el almacén de instancias)

Siga el procedimiento anterior hasta el paso en el que detiene la instancia. Cree una nueva AMI tal como se describe en Crear una AMI de Linux con respaldo en el almacén de instancias, asegurándose de habilitar el atributo de redes mejoradas cuando registre la AMI.

AWS CLI

register-image (AWS CLI/AWS CloudShell)

```
aws ec2 register-image --sriov-net-support simple ...
```

PowerShell

Register-EC2Image (AWS Tools for Windows PowerShell)

```
Register-EC2Image -SriovNetSupport "simple" ...
```

Windows

Si ha iniciado su instancia y no tiene habilitadas aún las redes mejoradas, debe descargar e instalar el controlador del adaptador de red requerido en la instancia y luego establecer el atributo de la instancia `sriovNetSupport` para activar las redes mejoradas. Solo puede habilitar este atributo

en tipos de instancias admitidos. Para obtener más información, consulte Se ha mejorado la compatibilidad de red.

> **Important**
>
> Para ver las actualizaciones de controladores más recientes en las AMI de Windows, consulte el historial de versiones de la AMI de Windows en la Referencia de las AMI de Windows de AWS.

Para habilitar las redes mejoradas

1. Conéctese a la instancia e inicie sesión como administrador local.
2. [Windows Server 2016 y versiones posteriores] Ejecute el siguiente script de PowerShell de EC2Launch para configurar la instancia después de instalar el controlador.

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
Schedule
```

> **Important**
>
> La contraseña del administrador se restablecerá cuando habilite el script de inicialización EC2Launch de la instancia. Puede modificar el archivo de configuración para deshabilitar el restablecimiento de la contraseña del administrador especificándolo en la configuración de las tareas de inicialización.

3. Desde la instancia, descargue el controlador del adaptador de red Intel para su sistema operativo:

   - Windows Server 2022

     Visite la página de descarga y descargue `Wired_driver_`*`version`*`_x64.zip`.
   - Windows Server 2019 incluida para versión de Server 1809 y posteriores*

     Visite la página de descarga y descargue `Wired_driver_`*`version`*`_x64.zip`.
   - Windows Server 2016 incluida para versión de Server 1803 y anteriores*

     Visite la página de descarga y descargue `Wired_driver_`*`version`*`_x64.zip`.

- Windows Server 2012 R2

  Visite la página de descarga y descargue `Wired_driver_version_x64.zip`.

- Windows Server 2012

  Visite la página de descarga y descargue `Wired_driver_version_x64.zip`.

- Windows Server 2008 R2

  Visite la página de descarga y descargue `PROWinx64Legacy.exe`.

*Las versiones de Server 1803 y anteriores, así como 1809 y posteriores no se tratan específicamente en las páginas de software y controladores de Intel.

4. Instale el controlador del adaptador de red Intel para su sistema operativo.

   - Windows Server 2008 R2

     1. En la carpeta Descargas, busque el archivo `PROWinx64Legacy.exe` y cámbiele el nombre a `PROWinx64Legacy.zip`.
     2. Extraiga el contenido del archivo `PROWinx64Legacy.zip`.
     3. Abra la línea de comandos, vaya a la carpeta que extrajo y ejecute el siguiente comando para utilizar la utilidad `pnputil` para agregar e instalar el archivo INF en el almacén de controladores.

        ```
        C:\> pnputil -a PROXGB\Winx64\NDIS62\vxn62x64.inf
        ```

   - Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2 y Windows Server 2012

     1. En la carpeta Descargas, extraiga el contenido del archivo `Wired_driver_version_x64.zip`.
     2. En la carpeta que extrajo, busque el archivo `Wired_driver_version_x64.exe` y cámbiele el nombre a `Wired_driver_version_x64.zip`.
     3. Extraiga el contenido del archivo `Wired_driver_version_x64.zip`.
     4. Abra la línea de comandos, vaya a la carpeta que extrajo y ejecute uno de los siguientes comandos para utilizar la utilidad `pnputil` para agregar e instalar el archivo INF en el almacén de controladores.

        - Windows Server 2022

```
C:\> pnputil -i -a PROXGB\Winx64\WS2022\vxs.inf
```

- Windows Server 2019

```
C:\> pnputil -i -a PROXGB\Winx64\NDIS68\vxn68x64.inf
```

- Windows Server 2016

```
C:\> pnputil -i -a PROXGB\Winx64\NDIS65\vxn65x64.inf
```

- Windows Server 2012 R2

```
C:\> pnputil -i -a PROXGB\Winx64\NDIS64\vxn64x64.inf
```

- Windows Server 2012

```
C:\> pnputil -i -a PROXGB\Winx64\NDIS63\vxn63x64.inf
```

5. En el equipo local, habilite el atributo de redes mejoradas con uno de los siguientes comandos:

   AWS CLI

   modify-instance-attribute (AWS CLI/AWS CloudShell)

   ```
   aws ec2 modify-instance-attribute --instance-id instance_id --sriov-net-support
    simple
   ```

   PowerShell

   Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

   ```
   Edit-EC2InstanceAttribute -InstanceId instance_id -SriovNetSupport "simple"
   ```

6. (Opcional) Cree una AMI desde la instancia, tal y como se explica en Creación de una AMI basada en Amazon EBS. La AMI hereda el atributo de redes mejoradas de la instancia. Por lo tanto, puede utilizar esta AMI para iniciar otra instancia con las redes mejoradas habilitadas de manera predeterminada.
7. Desde su equipo local, inicie la instancia mediante la consola de Amazon EC2 o uno de los siguientes comandos: start-instances (AWS CLI), Start-EC2Instance (AWS Tools for Windows

PowerShell). Si la instancia la administra AWS OpsWorks, debe iniciarla en la consola de AWS OpsWorks para mantener su estado sincronizado.

Solucionar problemas de conectividad

Si pierde la conexión mientras habilita las redes mejoradas, puede ser que el módulo `ixgbevf` sea incompatible con el kernel. Pruebe a instalar la versión del módulo `ixgbevf` que se incluye con la distribución de Linux de la instancia.

Si habilita las redes mejoradas para una instancia o AMI PV, la instancia podría ser inaccesible.

Para obtener más información, consulte How do I turn on and configure enhanced networking on my EC2 instances?

Monitoreo del rendimiento de la red de la instancia de EC2

El controlador de Elastic Network Adapter (ENA) publica métricas de rendimiento de la red desde las instancias en las que están habilitadas. Puede utilizar estas métricas para solucionar problemas de rendimiento de instancias, elegir el tamaño de instancia adecuado para una carga de trabajo, planificar actividades de escalado de forma proactiva y comparar las aplicaciones a fin de determinar si maximizan el rendimiento disponible en una instancia.

Amazon EC2 define los máximos de red en el nivel de instancia para garantizar una experiencia de redes de alta calidad, incluido un rendimiento de red constante en todos los tamaños de instancia. AWS proporciona máximos de lo siguiente para cada instancia:

- Capacidad de ancho de banda: cada instancia de EC2 tiene un ancho de banda máximo para el tráfico entrante y saliente agregado, según el tamaño y el tipo de instancias. Algunas instancias utilizan un mecanismo de créditos de E/S de red para asignar el ancho de banda de la red en función del uso de ancho de banda medio. Amazon EC2 también tiene un ancho de banda máximo para el tráfico hacia AWS Direct Connect e Internet. Para obtener más información, consulte Ancho de banda de red de instancias de Amazon EC2.
- Rendimiento de paquete por segundo (PPS): cada instancia de EC2 tiene un rendimiento de PPS máximo, según el tamaño y el tipo de instancias.
- Conexiones rastreadas: el grupo de seguridad realiza el seguimiento de cada conexión establecida para asegurarse de que los paquetes devueltos se entreguen como se espera. Existe un número máximo de conexiones que se pueden rastrear por instancia. Para obtener más información, consulte Seguimiento de conexiones de grupos de seguridad

- El acceso al servicio de enlace local: Amazon EC2 proporciona un PPS máximo por interfaz de red para el tráfico a servicios como el servicio de DNS, el servicio de metadatos de instancia y el Servicio de sincronización temporal de Amazon.

Cuando el tráfico de red de una instancia supera un máximo, AWS da forma al tráfico que supera el máximo al poner en cola y, a continuación, soltar paquetes de red. Puede monitorear cuando el tráfico supera un máximo mediante las métricas de rendimiento de la red. Estas métricas informan, en tiempo real, el impacto en el tráfico de red y los posibles problemas de rendimiento de la red.

Contenido

Requisitos

instancias de Linux

- Instale el controlador de ENA de versión 2.2.10 o posterior. Para verificar la versión instalada, utilice el comando ethtool. En el siguiente ejemplo, la versión cumple el requisito mínimo.

```
[ec2-user ~]$ ethtool -i eth0 | grep version
version: 2.2.10
```

  Para actualizar el controlador de ENA, consulte Red mejorada.
- Para importar estas métricas a Amazon CloudWatch, instale el agente CloudWatch. Para obtener más información, consulte Recopilar métricas de rendimiento de la red en Guía del usuario de Amazon CloudWatch.
- Para que tenga compatibilidad con la métrica `conntrack_allowance_available`, instale la versión 2.8.1 del controlador ENA.

instancias de Windows

- Instale el controlador de ENA de versión 2.2.2 o posterior. Para verificar la versión instalada, utilice el administrador de dispositivos de la siguiente manera.
  1. Abra el administrador de dispositivos mediante la ejecución de `devmgmt.msc`.
  2. Expanda Adaptadores de red.
  3. Elija Amazon Elastic Network Adapter, Propiedades.
  4. En la pestaña Controlador, busque Versión del controlador.

  Para actualizar el controlador de ENA, consulte Red mejorada.
- Para importar estas métricas a Amazon CloudWatch, instale el agente CloudWatch. Para obtener más información, consulte Recopilar métricas avanzadas de red en Guía del usuario de Amazon CloudWatch.

Métricas para el controlador de ENA

El controlador de ENA entrega las siguientes métricas a la instancia en tiempo real. Proporcionan el número acumulado de paquetes en cola o eliminado en cada interfaz de red desde el último restablecimiento del controlador.

Métrica	Descripción	Compatible con
`bw_in_allowance_exceeded`	El número de paquetes formados en cola o eliminados el ancho de banda agregado entrante superó el máximo de la instancia.	Todos los tipos de instancias
`bw_out_allowance_exceeded`	El número de paquetes en cola o eliminados porque el ancho de banda agregado saliente superó el máximo de la instancia.	Todos los tipos de instancias
`conntrack_allowance_exceeded`	El número de paquetes eliminados porque el seguimiento de conexiones superó el máximo de la instancia y no se pudieron establecer	Todos los tipos de instancias

Métrica	Descripción	Compatible con
	nuevas conexiones. Esto puede provocar la pérdida de paquetes para el tráfico hacia o desde la instancia.	
`conntrack_allowance_available`	La cantidad de conexiones rastreadas que puede establecer la instancia antes de alcanzar el límite de conexiones rastreadas de ese tipo de instancia.	Solo instancias integradas en AWS Nitro System
`linklocal_allowance_exceeded`	El número de paquetes eliminados porque el PPS del tráfico a los servicios proxy locales superó el máximo para la interfaz de red. Esto afecta al tráfico hacia el servicio de DNS, el servicio de metadatos de instancia y el Servicio de sincronización temporal de Amazon.	Todos los tipos de instancias
`pps_allowance_exceeded`	El número de paquetes en cola o eliminados porque el PPS bidireccional superó el máximo de la instancia.	Todos los tipos de instancias

Ver las métricas de rendimiento de la red de la instancia de

El procedimiento que utiliza depende del sistema operativo de la instancia.

instancias de Linux

Puede publicar métricas en sus herramientas favoritas para visualizar los datos de métricas. Por ejemplo, puede publicar las métricas en Amazon CloudWatch mediante el agente de CloudWatch. El agente permite seleccionar métricas individuales y controlar la publicación.

También puede utilizar ethtool para recuperar las métricas de cada interfaz de red, como eth0, de la siguiente manera.

```
[ec2-user ~]$ ethtool -S eth0
     bw_in_allowance_exceeded: 0
     bw_out_allowance_exceeded: 0
     pps_allowance_exceeded: 0
     conntrack_allowance_exceeded: 0
     linklocal_allowance_exceeded: 0
     conntrack_allowance_available: 136812
```

instancias de Windows

Puede ver las métricas con cualquier consumidor de contadores de rendimiento de Windows. Los datos se pueden analizar de acuerdo con el manifiesto EnaPerfCounters. Este es un archivo XML que define el proveedor de contador de rendimiento y sus conjuntos de contadores.

Para instalar el manifiesto

Si ha iniciado la instancia con una AMI que contiene el controlador de ENA 2.2.2 o posterior o utilizado el script de instalación en el paquete de controladores para el controlador de ENA 2.2.2, el manifiesto ya está instalado. Para instalar el manifiesto manualmente, siga los pasos siguientes:

1. Elimine el manifiesto existente mediante el siguiente comando:

   ```
   unlodctr /m:EnaPerfCounters.man
   ```

2. Copie el archivo del manifiesto, `EnaPerfCounters.man`, del paquete de instalación del controlador a `%SystemRoot%\System32\drivers`.
3. Instale el nuevo manifiesto mediante el siguiente comando:

   ```
   lodctr /m:EnaPerfCounters.man
   ```

Para ver métricas mediante el Monitor de rendimiento

1. Abra el Monitor de rendimiento.
2. Presione Ctrl+N para agregar nuevos contadores.
3. Elija Configuración de paquetes de ENA en la lista.
4. Seleccione las instancias que desea monitorear y elija Agregar.

5. Seleccione OK.

Métricas para ENA Express

ENA Express funciona con la tecnología Scalable Reliable Datagram (SRD) de AWS. SRD es un protocolo de transporte de red de alto rendimiento que utiliza el enrutamiento dinámico para aumentar el rendimiento y minimizar la latencia de cola. Puede utilizar las métricas de ENA Express para asegurarse de que sus instancias aprovechen al máximo las mejoras de rendimiento que proporciona la tecnología SRD, por ejemplo:

- Evalúe sus recursos para asegurarse de que tengan capacidad suficiente para establecer más conexiones de SRD.
- Identifique dónde hay posibles problemas que impidan que los paquetes salientes aptos utilicen SRD.
- Calcule el porcentaje de tráfico saliente que usa SRD para la instancia.
- Calcule el porcentaje de tráfico entrante que usa SRD para la instancia.

> **Note**
>
> Para generar métricas, utilice la versión 2.8 o superior del controlador.

Las siguientes métricas de ENA Express están disponibles mediante el comando ethtool para instancias basadas en Linux.

- `ena_srd_mode`: describe qué características de ENA Express están habilitadas. Los valores son los siguientes:
  - `0` = ENA Express desactivado, UDP desactivado
  - `1` = ENA Express activado, UDP desactivado
  - `2` = ENA Express desactivado, UDP activado

    > **Note**
    >
    > Esto solo ocurre cuando ENA Express se habilitó originalmente y UDP se configuró para usarlo. El valor anterior se retiene para el tráfico UDP.

  - 3 = ENA Express activado, UDP activado
- `ena_srd_eligible_tx_pkts`: el número de paquetes de red enviados dentro de un periodo de tiempo determinado que cumplen los requisitos de SRD, como se indica a continuación:
  - Se admiten los tipos de instancia de envío y recepción. Para obtener más información, consulte la tabla Tipos de instancia compatibles con ENA Express.
  - Tanto las instancias de envío como las de recepción deben tener configurado ENA Express.
  - Las instancias de envío y recepción deben ejecutarse en la misma zona de disponibilidad.
  - La ruta de red entre las instancias no debe incluir cajas de middleware. ENA Express no admite actualmente cajas de middleware.

> **Note**
>
> La métrica de elegibilidad de ENA Express abarca los requisitos de origen y destino, y la red entre los dos puntos de conexión. Los paquetes aptos aún pueden ser descalificados tras su recuento. Por ejemplo, si un paquete apto supera el límite de la unidad de transmisión máxima (MTU), vuelve a la transmisión ENA estándar, aunque el paquete se sigue mostrando como apto en el contador.

- `ena_srd_tx_pkts`: el número de paquetes SRD transmitidos en un periodo de tiempo determinado.
- `ena_srd_rx_pkts`: el número de paquetes SRD recibidos en un periodo de tiempo determinado.
- `ena_srd_resource_utilization`: el porcentaje de uso máximo de memoria permitido para conexiones SRD simultáneas que ha consumido la instancia.

Para ver una lista de las métricas que se filtran para ENA Express, ejecute el siguiente comando ethtool para su interfaz de red (que aquí se muestra como `eth0`):

```
[ec2-user ~]$ ethtool -S eth0 | grep ena_srd
NIC statistics:
 ena_srd_mode: 0
 ena_srd_tx_pkts: 0
 ena_srd_eligible_tx_pkts: 0
 ena_srd_rx_pkts: 0
 ena_srd_resource_utilization: 0
```

Tráfico de salida (paquetes salientes)

Para asegurarse de que su tráfico de salida utiliza SRD como se espera, compare el número de paquetes SRD aptos (`ena_srd_eligible_tx_pkts`) con el número de paquetes SRD enviados (`ena_srd_tx_pkts`) durante un periodo de tiempo determinado.

Las diferencias significativas entre el número de paquetes aptos y el número de paquetes SRD enviados suelen deberse a problemas de utilización de recursos. Cuando la tarjeta de red conectada a la instancia agota sus recursos máximos, o si los paquetes superan el límite de MTU, los paquetes aptos no pueden transmitirse a través de SRD y deben volver a la transmisión ENA estándar. Los paquetes también pueden experimentar esto durante migraciones en directo o actualizaciones de servidores en directo. Se requiere una solución de problemas adicionales para determinar la causa raíz.

> **Note**
>
> Puede ignorar las pequeñas diferencias ocasionales entre el número de paquetes aptos y el número de paquetes de SRD. Esto puede ocurrir cuando su instancia establece una conexión con otra instancia para el tráfico SRD, por ejemplo.

Para averiguar qué porcentaje de su tráfico de salida total durante un periodo de tiempo determinado utiliza SRD, compare el número de paquetes SRD enviados (`ena_srd_tx_pkts`) con el número total de paquetes enviados para la instancia (`NetworkPacketOut`) durante ese tiempo.

Tráfico de entrada (paquetes entrantes)

Para saber qué porcentaje del tráfico de entrada utiliza SRD, compare el número de paquetes SRD recibidos (`ena_srd_rx_pkts`) durante un periodo de tiempo determinado con el número total de paquetes recibidos para la instancia (`NetworkPacketIn`) durante ese tiempo.

Uso de los recursos

El uso de los recursos se basa en el número de conexiones SRD simultáneas que una única instancia puede mantener en un momento determinado. La métrica de uso de recursos (`ena_srd_resource_utilization`) hace un seguimiento del uso actual de la instancia. A medida que la utilización se acerque al 100 %, es de esperar que se produzcan problemas de rendimiento. ENA Express retrocede de la transmisión SRD a la transmisión ENA estándar y aumenta la posibilidad de que se pierdan paquetes. Un alto uso de recursos es un indicio de que llegó el momento de escalar horizontalmente la instancia para mejorar el rendimiento de la red.

> **Note**
>
> Cuando el tráfico de red de una instancia supera un máximo, AWS da forma al tráfico que supera el máximo al poner en cola y, a continuación, soltar paquetes de red.

Persistencia

Las métricas de entrada y salida se acumulan mientras ENA Express está habilitado para la instancia. Las métricas dejan de acumularse si ENA Express está desactivado, pero persisten mientras la instancia sigue en ejecución. Las métricas se reinician si la instancia se reinicia o se finaliza, o si la interfaz de red se desvincula de la instancia.

Métricas de rendimiento de la red con el controlador de DPDK para ENA

El controlador de ENA, versión 2.2.0 y posterior, admite informes de métricas de red. DPDK 20.11 incluye el controlador de ENA 2.2.0 y es la primera versión de DPDK que admite esta característica.

Puede utilizar una aplicación de ejemplo para ver las estadísticas de DPDK. Para comenzar una versión interactiva de la aplicación de ejemplo, ejecute el siguiente comando.

```
./app/dpdk-testpmd -- -i
```

Dentro de esta sesión interactiva, puede escribir un comando para recuperar estadísticas extendidas de un puerto. El siguiente comando de ejemplo recupera las estadísticas del puerto 0.

```
show port xstats 0
```

A continuación se muestra un ejemplo de una sesión interactiva con la aplicación de ejemplo de DPDK.

```
[root@ip-192.0.2.0 build]# ./app/dpdk-testpmd -- -i
        EAL: Detected 4 lcore(s)
        EAL: Detected 1 NUMA nodes
        EAL: Multi-process socket /var/run/dpdk/rte/mp_socket
        EAL: Selected IOVA mode 'PA'
        EAL: Probing VFIO support...
        EAL:   Invalid NUMA socket, default to 0
        EAL:   Invalid NUMA socket, default to 0
        EAL: Probe PCI driver: net_ena (1d0f:ec20) device: 0000:00:06.0
(socket 0)
```

```
        EAL: No legacy callbacks, legacy socket not created
        Interactive-mode selected

        Port 0: link state change event
        testpmd: create a new mbuf pool <mb_pool_0>: n=171456,
size=2176, socket=0
        testpmd: preferred mempool ops selected: ring_mp_mc

        Warning! port-topology=paired and odd forward ports number, the
last port will pair with itself.

        Configuring Port 0 (socket 0)
        Port 0: 02:C7:17:A2:60:B1
        Checking link statuses...
        Done
        Error during enabling promiscuous mode for port 0: Operation
not supported - ignore
        testpmd> show port xstats 0
        ###### NIC extended statistics for port 0
        rx_good_packets: 0
        tx_good_packets: 0
        rx_good_bytes: 0
        tx_good_bytes: 0
        rx_missed_errors: 0
        rx_errors: 0
        tx_errors: 0
        rx_mbuf_allocation_errors: 0
        rx_q0_packets: 0
        rx_q0_bytes: 0
        rx_q0_errors: 0
        tx_q0_packets: 0
        tx_q0_bytes: 0
        wd_expired: 0
        dev_start: 1
        dev_stop: 0
        tx_drops: 0
        bw_in_allowance_exceeded: 0
        bw_out_allowance_exceeded: 0
        pps_allowance_exceeded: 0
        conntrack_allowance_exceeded: 0
        linklocal_allowance_exceeded: 0
        rx_q0_cnt: 0
        rx_q0_bytes: 0
        rx_q0_refill_partial: 0
```

```
        rx_q0_bad_csum: 0
        rx_q0_mbuf_alloc_fail: 0
        rx_q0_bad_desc_num: 0
        rx_q0_bad_req_id: 0
        tx_q0_cnt: 0
        tx_q0_bytes: 0
        tx_q0_prepare_ctx_err: 0
        tx_q0_linearize: 0
        tx_q0_linearize_failed: 0
        tx_q0_tx_poll: 0
        tx_q0_doorbells: 0
        tx_q0_bad_req_id: 0
        tx_q0_available_desc: 1023
        testpmd>
```

Para obtener más información acerca de la aplicación de ejemplo y su uso a fin de recuperar estadísticas ampliadas. consulte la Guía del usuario de la aplicación de Testpmd en la documentación de DPDK.

Métricas en instancias que ejecutan FreeBSD

A partir de la versión 2.3.0, el controlador FreeBSD de ENA admite la recopilación de métricas de rendimiento de la red en instancias que ejecutan FreeBSD. Para habilitar la recopilación de métricas de FreeBSD, ingrese el siguiente comando y establezca el *intervalo* en un valor entre 1 y 3600. Esto especifica la frecuencia, en segundos, para recopilar métricas de FreeBSD.

```
sysctl dev.ena.network_interface.eni_metrics.sample_interval=interval
```

Por ejemplo, el siguiente comando configura el controlador para recopilar métricas de FreeBSD en la interfaz de red 1 cada 10 segundos:

```
sysctl dev.ena.1.eni_metrics.sample_interval=10
```

Para desactivar la recopilación de métricas de FreeBSD puede ejecutar el comando anterior y especificar `0` como *intervalo*.

Después de habilitar la recopilación de métricas de FreeBSD, puede recuperar el último conjunto de métricas recopiladas mediante la ejecución del siguiente comando.

```
sysctl dev.ena.network_interface.eni_metrics
```

Solución de problemas de Elastic Network Adapter en Linux

Elastic Network Adapter (ENA) se ha diseñado para mejorar la salud del sistema operativo y reducir la posibilidad de interrupción a largo plazo debido a errores o a comportamientos de hardware inesperados. La arquitectura ENA mantiene los errores de la unidad o el dispositivo lo más transparente posible para el sistema. En este tema se proporciona información sobre cómo solucionar problemas de ENA.

Si no puede conectarse a la instancia, comience por la sección Solucionar problemas de conectividad.

Si experimenta una degradación del rendimiento después de migrar a un tipo de instancia de sexta generación, consulte el artículo What do I need to do before I migrate my EC2 instance to a sixth generation instance to make sure that I get maximum network performance?

Si puede conectarse a la instancia, puede recopilar la información de diagnóstico usando la detección de errores y los mecanismos de recuperación que se abordan en secciones posteriores dentro de este tema.

Contenido

Solucionar problemas de conectividad

Si pierde la conexión mientras habilita la red mejorada, puede ser que el módulo `ena` sea incompatible con el kernel en ejecución de la instancia. Esto puede ocurrir si instala el módulo para una versión de kernel específica (sin dkms o con un archivo dkms.conf incorrectamente configurado) y después se actualiza el kernel de la instancia. Si el kernel de la instancia que está cargado al arrancar no tiene un módulo `ena` correctamente instalado, la instancia no reconocerá el adaptador de red y la instancia no será alcanzable.

Habilitar las redes mejoradas para una instancia o AMI de PV también puede hacer que la instancia no sea alcanzable.

Si la instancia no es alcanzable después de habilitar las redes mejoradas con ENA, puede deshabilitar el atributo `enaSupport` de la instancia y volverá al adaptador de red.

Para inhabilitar las redes mejoradas con ENA (instancias respaldadas por EBS)

1. En la computadora local, detenga la instancia usando la consola de Amazon EC2 o uno de los siguientes comandos: stop-instances (AWS CLI), Stop-EC2Instance (AWS Tools for Windows PowerShell). Si la instancia la administra AWS OpsWorks, debe detenerla en la consola de AWS OpsWorks para mantener su estado sincronizado.

   > **Important**
   >
   > Si usa una instancia respaldada por un almacén de instancias, no podrá pararla. En lugar de esto, siga con Para deshabilitar las redes mejoradas con ENA (instancias con respaldo en el almacenamiento de la instancia).

2. En el equipo local, deshabilite el atributo de redes mejoradas con el siguiente comando.

   - modify-instance-attribute (AWS CLI)

     ```
     $ C:\> aws ec2 modify-instance-attribute --instance-id instance_id --no-ena-support
     ```

3. En la computadora local, inicie la instancia usando la consola de Amazon EC2 o uno de los siguientes comandos: start-instances (AWS CLI), Start-EC2Instance (AWS Tools for Windows PowerShell). Si la instancia la administra AWS OpsWorks, debe iniciarla en la consola de AWS OpsWorks para mantener su estado sincronizado.
4. (Opcional) Conéctese a la instancia e intente reinstalar el módulo `ena` con la versión de kernel actual siguiendo los pasos de Habilitación de las redes mejoradas con Elastic Network Adapter (ENA) en las instancias EC2.

Para deshabilitar las redes mejoradas con ENA (instancias con respaldo en el almacenamiento de la instancia)

Si la suya es una instancia respaldada por un almacén de instancias, cree una nueva AMI como se describe en Crear una AMI de Linux con respaldo en el almacén de instancias. Asegúrese de deshabilitar el atributo `enaSupport` de redes mejoradas cuando registre la AMI.

- register-image (AWS CLI)

```
$ C:\> aws ec2 register-image --no-ena-support ...
```

- Register-EC2Image (AWS Tools for Windows PowerShell)

```
C:\> Register-EC2Image -EnaSupport $false ...
```

Mecanismo Keep-alive

El dispositivo ENA publica eventos keep-alive a intervalos establecidos (por lo general una vez por segundo). El controlador de ENA implementa un mecanismo watchdog para detectar la presencia de estos mensajes keep-alive. Si hay uno o varios mensajes, el watchdog se rearma; de lo contrario, el controlador concluye que el dispositivo experimentó un error y hace lo siguiente:

- Vuelca las estadísticas actuales en el syslog
- Restablece el dispositivo ENA
- Restablece el estado del controlador ENA

El procedimiento anterior puede dar lugar a cierta pérdida de tráfico durante un breve periodo (las conexiones TCP deberían poder recuperarse), pero no debería afectar al usuario en nada más.

El dispositivo ENA también puede solicitar indirectamente un procedimiento de restablecimiento de dispositivos, no enviando una notificación keep-alive, por ejemplo, si el dispositivo de ENA llega a un estado desconocido después de cargar una configuración irrecuperable.

El siguiente es un ejemplo del procedimiento de restablecimiento:

```
[18509.800135] ena 0000:00:07.0 eth1: Keep alive watchdog timeout. // The watchdog
 process initiates a reset
[18509.815244] ena 0000:00:07.0 eth1: Trigger reset is on
[18509.825589] ena 0000:00:07.0 eth1: tx_timeout: 0 // The driver logs the current
 statistics
[18509.834253] ena 0000:00:07.0 eth1: io_suspend: 0
[18509.842674] ena 0000:00:07.0 eth1: io_resume: 0
[18509.850275] ena 0000:00:07.0 eth1: wd_expired: 1
[18509.857855] ena 0000:00:07.0 eth1: interface_up: 1
[18509.865415] ena 0000:00:07.0 eth1: interface_down: 0
[18509.873468] ena 0000:00:07.0 eth1: admin_q_pause: 0
[18509.881075] ena 0000:00:07.0 eth1: queue_0_tx_cnt: 0
```

```
[18509.888629] ena 0000:00:07.0 eth1: queue_0_tx_bytes: 0
[18509.895286] ena 0000:00:07.0 eth1: queue_0_tx_queue_stop: 0
.......
........
[18511.280972] ena 0000:00:07.0 eth1: free uncompleted tx skb qid 3 idx 0x7 // At the
 end of the down process, the driver discards incomplete packets.
[18511.420112] [ENA_COM: ena_com_validate_version] ena device version: 0.10 //The
 driver begins its up process
[18511.420119] [ENA_COM: ena_com_validate_version] ena controller version: 0.0.1
 implementation version 1
[18511.420127] [ENA_COM: ena_com_admin_init] ena_defs : Version:[b9692e8] Build date
 [Wed Apr  6 09:54:21 IDT 2016]
[18512.252108] ena 0000:00:07.0: Device watchdog is Enabled
[18512.674877] ena 0000:00:07.0: irq 46 for MSI/MSI-X
[18512.674933] ena 0000:00:07.0: irq 47 for MSI/MSI-X
[18512.674990] ena 0000:00:07.0: irq 48 for MSI/MSI-X
[18512.675037] ena 0000:00:07.0: irq 49 for MSI/MSI-X
[18512.675085] ena 0000:00:07.0: irq 50 for MSI/MSI-X
[18512.675141] ena 0000:00:07.0: irq 51 for MSI/MSI-X
[18512.675188] ena 0000:00:07.0: irq 52 for MSI/MSI-X
[18512.675233] ena 0000:00:07.0: irq 53 for MSI/MSI-X
[18512.675279] ena 0000:00:07.0: irq 54 for MSI/MSI-X
[18512.772641] [ENA_COM: ena_com_set_hash_function] Feature 10 isn't supported
[18512.772647] [ENA_COM: ena_com_set_hash_ctrl] Feature 18 isn't supported
[18512.775945] ena 0000:00:07.0: Device reset completed successfully // The reset
 process is complete
```

Registrar tiempo de espera de lectura

La arquitectura de ENA sugiere un uso limitado de operaciones de lectura I/O mapeadas a la memoria, MMIO. El controlador del dispositivo de ENA tiene acceso a los registros de MMIO solo durante el procedimiento de inicialización.

Si los logs del controlador (disponibles en el resultado de dmesg) indican errores en las operaciones de lectura, puede ser debido a un controlador incompatible o compilado incorrectamente, un dispositivo de hardware ocupado o un error de hardware.

Las entradas de registro intermitentes que indican errores en operaciones de lectura no deben considerarse un problema, el controlador volverá a intentarlas en este caso. Sin embargo, una secuencia de entradas de registro que contenga errores de lectura indica un problema de controlador o de hardware.

A continuación se ofrece un ejemplo de una entrada de registro de controlador que indica un error en una operación de lectura debido a un tiempo de espera:

```
[ 47.113698] [ENA_COM: ena_com_reg_bar_read32] reading reg failed for timeout.
 expected: req id[1] offset[88] actual: req id[57006] offset[0]
[ 47.333715] [ENA_COM: ena_com_reg_bar_read32] reading reg failed for timeout.
 expected: req id[2] offset[8] actual: req id[57007] offset[0]
[ 47.346221] [ENA_COM: ena_com_dev_reset] Reg read32 timeout occurred
```

Statistics

Si experimente problemas de latencia o rendimiento de red insuficiente, recupere las estadísticas del dispositivo y examínelas. Estas estadísticas se obtienen mediante ethtool, como se muestra abajo:

```
[ec2-user ~]$ ethtool -S ethN
NIC statistics:
 tx_timeout: 0
 suspend: 0
 resume: 0
 wd_expired: 0
 interface_up: 1
 interface_down: 0
 admin_q_pause: 0
 bw_in_allowance_exceeded: 0
 bw_out_allowance_exceeded: 0
 pps_allowance_exceeded: 0
 conntrack_allowance_available: 450878
 conntrack_allowance_exceeded: 0
 linklocal_allowance_exceeded: 0
 queue_0_tx_cnt: 4329
 queue_0_tx_bytes: 1075749
 queue_0_tx_queue_stop: 0
 ...
```

Los parámetros de resultado del siguiente comando se describen a continuación:

`tx_timeout`: *N*

El número de veces que se activó el watchdog Netdev.

`suspend`: *N*

El número de veces que el controlador realizó una operación de suspensión.

`resume`: *N*

El número de veces que el controlador realizó una operación de reanudación.

`wd_expired`: *N*

El número de veces que el controlador no recibió el evento keep-alive en los tres segundos anteriores.

`interface_up`: *N*

El número de veces que se activó la interfaz de ENA.

`interface_down`: *N*

El número de veces que se desactivó la interfaz de ENA.

`admin_q_pause`: *N*

El número de veces que la cola de administración no se encontró en un estado de ejecución.

`bw_in_allowance_exceeded`: *N*

El número de paquetes formados en cola o eliminados el ancho de banda agregado entrante superó el máximo de la instancia.

`bw_out_allowance_exceeded`: *N*

El número de paquetes en cola o eliminados porque el ancho de banda agregado saliente superó el máximo de la instancia.

`pps_allowance_exceeded`: *N*

El número de paquetes en cola o eliminados porque el PPS bidireccional superó el máximo de la instancia.

`conntrack_allowance_available`: *N*

La cantidad de conexiones rastreadas que puede establecer la instancia antes de alcanzar el límite de conexiones rastreadas de ese tipo de instancia. Solo disponible para instancias basadas en Nitro. No compatibles con instancias de FreeBSD ni con entornos de DPDK.

`conntrack_allowance_exceeded`: *N*

El número de paquetes eliminados porque el seguimiento de conexiones superó el máximo de la instancia y no se pudieron establecer nuevas conexiones. Esto puede provocar la pérdida de paquetes para el tráfico hacia o desde la instancia.

`linklocal_allowance_exceeded`: *N*

El número de paquetes eliminados porque el PPS del tráfico a los servicios proxy locales superó el máximo para la interfaz de red. Esto afecta al tráfico hacia el servicio de DNS, el servicio de metadatos de instancia y el Servicio de sincronización temporal de Amazon.

`queue_`*N*`_tx_cnt`: *N*

El número de paquetes transmitidos para esta cola.

`queue_`*N*`_tx_bytes`: *N*

El número de bytes transmitidos para esta cola.

`queue_`*N*`_tx_queue_stop`: *N*

El número de veces que la cola *N* se llenó y se paró.

`queue_`*N*`_tx_queue_wakeup`: *N*

El número de veces que la cola *N* se reanudó después de pararse.

`queue_`*N*`_tx_dma_mapping_err`: *N*

Cuenta de errores de acceso directo a memoria. Si este valor no es 0, significa que los recursos del sistema están bajos.

`queue_`*N*`_tx_linearize`: *N*

El número de veces que se intentó la linearización SKB para esta cola.

`queue_`*N*`_tx_linearize_failed`: *N*

El número de veces que la linearización SKB para esta cola dio error.

`queue_`*N*`_tx_napi_comp`: *N*

El número de veces que el controlador `napi` llamó a `napi_complete` para esta cola.

`queue_`*N*`_tx_tx_poll`: *N*

El número de veces que el controlador `napi` se programó para esta cola.

`queue_`*N*`_tx_doorbells`: *N*

El número de timbres de transmisión para esta cola.

`queue_`*N*`_tx_prepare_ctx_err`: *N*

El número de veces que `ena_com_prepare_tx` dio error para esta cola.

`queue_N_tx_bad_req_id`: *N*

`req_id` no válido para esta cola. El `req_id` válido es cero, menos `queue_size`, menos 1.

`queue_N_tx_llq_buffer_copy`: *N*

El número de paquetes cuyo tamaño de encabezados es mayor que la entrada llq para esta cola.

`queue_N_tx_missed_tx`: *N*

El número de paquetes que quedaron incompletos para esta cola.

`queue_N_tx_unmask_interrupt`: *N*

El número de veces que se desenmascaró la interrupción de tx para esta cola.

`queue_N_rx_cnt`: *N*

El número de paquetes que se recibió para esta cola.

`queue_N_rx_bytes`: *N*

El número de bytes que se recibió para esta cola.

`queue_N_rx_rx_copybreak_pkt`: *N*

El número de veces que la cola rx recibió un paquete cuyo tamaño es menor que el del paquete rx_copybreak para esta cola.

`queue_N_rx_csum_good`: *N*

El número de veces que la cola rx recibió un paquete en el que se verificó la suma de comprobación y era correcta para esta cola.

`queue_N_rx_refil_partial`: *N*

El número de veces que el controlador no logró rellenar la porción vacía de la cola rx con los búferes para esta cola. Si este valor no es 0, indica que los recursos de memoria están bajos.

`queue_N_rx_bad_csum`: *N*

El número de veces que la cola `rx` tuvo una suma de comprobación incorrecta para esta cola (solo si se admite la descarga de la suma de comprobación de rx).

`queue_N_rx_page_alloc_fail`: *N*

El número de veces que la asignación de página para esta cola dio error. Si este valor no es 0, indica que los recursos de memoria están bajos.

`queue_N_rx_skb_alloc_fail`: *N*

El número de veces que la asignación de SKB para esta cola dio error. Si este valor no es 0, indica que los recursos del sistema están bajos.

`queue_N_rx_dma_mapping_err`: *N*

Cuenta de errores de acceso directo a memoria. Si este valor no es 0, significa que los recursos del sistema están bajos.

`queue_N_rx_bad_desc_num`: *N*

Demasiados búferes por paquete. Si este valor no es 0, indica el uso de búferes muy pequeños.

`queue_N_rx_bad_req_id`: *N*

El req_id para esta cola no es válido. El req_id válido es de [0, queue_size - 1].

`queue_N_rx_empty_rx_ring`: *N*

El número de veces que la cola rx estuvo vacía para esta cola.

`queue_N_rx_csum_unchecked`: *N*

El número de veces que la cola rx recibió un paquete cuya suma de comprobación no se verificó para esta cola.

`queue_N_rx_xdp_aborted`: *N*

El número de veces que un paquete XDP se clasificó como XDP_ABORT.

`queue_N_rx_xdp_drop`: *N*

El número de veces que un paquete XDP se clasificó como XDP_DROP.

`queue_N_rx_xdp_pass`: *N*

El número de veces que un paquete XDP se clasificó como XDP_PASS.

`queue_N_rx_xdp_tx`: *N*

El número de veces que un paquete XDP se clasificó como XDP_TX.

`queue_N_rx_xdp_invalid`: *N*

El número de veces que el código devuelto XDP para el paquete no era válido.

`queue_N_rx_xdp_redirect`: *N*

El número de veces que un paquete XDP se clasificó como XDP_REDIRECT.

`queue_N_xdp_tx_cnt`: *N*

El número de paquetes transmitidos para esta cola.

`queue_N_xdp_tx_bytes`: *N*

El número de bytes transmitidos para esta cola.

`queue_N_xdp_tx_queue_stop`: *N*

El número de veces que esta cola se llenó y se detuvo.

`queue_N_xdp_tx_queue_wakeup`: *N*

El número de veces que esta cola se reanudó después de detenerse.

`queue_N_xdp_tx_dma_mapping_err`: *N*

Cuenta de errores de acceso directo a memoria. Si este valor no es 0, significa que los recursos del sistema están bajos.

`queue_N_xdp_tx_linearize`: *N*

El número de veces que se intentó la linealización del búfer XDP para esta cola.

`queue_N_xdp_tx_linearize_failed`: *N*

El número de veces que se produjo un error en la linealización del búfer XDP para esta cola.

`queue_N_xdp_tx_napi_comp`: *N*

El número de veces que el controlador napi llamó napi_complete para esta cola.

`queue_N_xdp_tx_tx_poll`: *N*

El número de veces que se programó el controlador napi para esta cola.

`queue_N_xdp_tx_doorbells`: *N*

El número de timbres de transmisión para esta cola.

`queue_N_xdp_tx_prepare_ctx_err`: *N*

El número de veces que ena_com_prepare_tx dio error para esta cola. Este valor debe ser siempre cero; si no es así, consulte los logs del controlador.

`queue_N_xdp_tx_bad_req_id`: *N*

El req_id para esta cola no es válido. El req_id válido es de [0, queue_size - 1].

`queue_N_xdp_tx_llq_buffer_copy`: *N*

El número de paquetes cuyos encabezados se copiaron usando la copia del búfer llq para esta cola.

`queue_N_xdp_tx_missed_tx`: *N*

El número de veces que una entrada de cola tx perdió un tiempo de espera de finalización para esta cola.

`queue_N_xdp_tx_unmask_interrupt`: *N*

El número de veces que se desenmascaró la interrupción de tx para esta cola.

`ena_admin_q_aborted_cmd`: *N*

El número total de comandos admin que se anularon. Esto sucede, por lo general, durante el procedimiento de autorrecuperación.

`ena_admin_q_submitted_cmd`: *N*

El número de timbres de cola admin.

`ena_admin_q_completed_cmd`: *N*

El número de finalizaciones de la cola admin.

`ena_admin_q_out_of_space`: *N*

El número de veces que el controlador intentó enviar un nuevo comando admin, pero la cola estaba llena.

`ena_admin_q_no_completion`: *N*

El número de veces que el controlador no logró una finalización admin para un comando.

Registros de errores de controlador en syslog

El controlador de ENA escribe mensajes de registro en syslog durante el arranque del sistema. Puede examinarlo para buscar errores si está experimentando problemas. A continuación puede ver un ejemplo de información registrada por el controlador de ENA en syslog durante el arranque del sistema, junto con algunas anotaciones para mensajes seleccionados.

```
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  478.416939] [ENA_COM:
 ena_com_validate_version] ena device version: 0.10
```

```
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  478.420915] [ENA_COM:
 ena_com_validate_version] ena controller version: 0.0.1 implementation version 1
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.256831] ena 0000:00:03.0: Device
 watchdog is Enabled
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.672947] ena 0000:00:03.0: creating 8 io
 queues. queue size: 1024
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.680885] [ENA_COM:
 ena_com_init_interrupt_moderation] Feature 20 isn't supported  // Interrupt moderation
 is not supported by the device
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.691609] [ENA_COM:
 ena_com_get_feature_ex] Feature 10 isn't supported // RSS HASH function configuration
 is not supported by the
 device
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.694583] [ENA_COM:
 ena_com_get_feature_ex] Feature 18 isn't supported //RSS HASH input source
 configuration is not supported by the device
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.697433] [ENA_COM:
 ena_com_set_host_attributes] Set host attribute isn't supported
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.701064] ena 0000:00:03.0 (unnamed
 net_device) (uninitialized): Cannot set host attributes
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.704917] ena 0000:00:03.0: Elastic
 Network Adapter (ENA) found at mem f3000000, mac addr 02:8a:3c:1e:13:b5 Queues 8
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  480.805037] EXT4-fs (xvda1): re-mounted.
 Opts: (null)
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  481.025842] NET: Registered protocol family
 10
```

¿Qué tipo de errores se puede omitir?

Las advertencias siguientes que aparecen en el registro de errores del sistema se puede omitir para ENA:

La configuración de atributos de host no es compatible

Los atributos de host no se admiten con este dispositivo.

Error al asignar un búfer para la cola de recepción (rx queue)

Este en un error recuperable que indica que podría haber habido una presión de memoria cuando se produjo.

La característica *X* no es compatible

La característica mencionada no es compatible con ENA. Entre los valores posibles para *X* se incluyen:

- **10**: la configuración de la función Hash de RSS no es compatible con este dispositivo.
- **12**: la configuración de la tabla de indirección de RSS no es compatible con este dispositivo.
- **18**: la configuración de la entrada de Hash de RSS no es compatible con este dispositivo.
- **20**: la moderación de interrupciones no es compatible con este dispositivo..
- **27**: el controlador del Elastic Network Adapter no admite sondear las capacidades de Ethernet desde snmpd.

La configuración de AENQ ha fallado

El ENA no es compatible con la configuración AENQ.

Intentando configurar eventos de AENQ no compatibles

Este error indica que se está intentando establecer un grupo de eventos de AENQ no admitido por ENA.

Notificaciones de configuración subóptimas

El dispositivo ENA detecta ajustes de configuración subóptimos en el controlador que usted puede cambiar. El dispositivo notifica al controlador ENA y registra una advertencia en la consola. En el ejemplo siguiente se muestra el formato del mensaje de advertencia.

```
Sub-optimal configuration notification code: 1. Refer to AWS ENA documentation for
 additional details and mitigation options.
```

La siguiente lista muestra los detalles del código de la notificación y las acciones recomendadas en caso de que la configuración no sea óptima.

- Código **1**: no se recomienda el uso de ENA Express con una configuración de LLQ amplio

  El ENI de ENA Express está configurado con un LLQ amplio. Esta configuración no es óptima y podría afectar al rendimiento de ENA Express. Le recomendamos que desactive la configuración de LLQ amplio cuando utilice los ENI de ENA Express de la siguiente manera.

  ```
  sudo rmmod ena && sudo modprobe ena force_large_llq_header=0
  ```

  Para obtener más información sobre la configuración óptima de ENA Express, consulte Mejora del rendimiento de la red con ENA Express en las instancias EC2.

- Código **2**: no se recomienda la ENI de ENA Express con una profundidad de cola de Tx inferior a la óptima

  La ENI de ENA Express está configurada con una profundidad de cola de Tx inferior a la óptima. Esta configuración podría afectar al rendimiento de ENA Express. Le recomendamos que amplíe todas las colas de Tx al valor máximo para la interfaz de red cuando utilice las ENI de ENA Express de la siguiente manera.

  Puede ejecutar los siguientes comandos ethtool para ajustar el tamaño de LLQ. Para obtener más información sobre cómo controlar, consultar y habilitar Wide-LLQ, consulte el tema Large Low-Latency Queue (Large LLQ) del controlador del kernel de Linux para la documentación ENA en el repositorio de GitHub de Amazon Drivers.

  ```
  ethtool -g interface
  ```

  Defina sus colas de Tx a la profundidad máxima:

  ```
  ethtool -G interface tx depth
  ```

  Para obtener más información sobre la configuración óptima de ENA Express, consulte Mejora del rendimiento de la red con ENA Express en las instancias EC2.

- Código **3**: ENA con un tamaño LLQ normal y un tráfico de paquetes de Tx que supera el tamaño máximo de encabezado admitido

  De forma predeterminada, ENA LLQ admite un tamaño de encabezado de paquete Tx de hasta 96 bytes. Si el tamaño del encabezado del paquete es superior a 96 bytes, el paquete se descarta. Para mitigar este problema, le recomendamos que habilite Wide-LLQ, que aumenta el tamaño del encabezado de paquete Tx admitido hasta un máximo de 224 bytes.

  Sin embargo, al activar Wide-LLQ, el tamaño máximo del anillo Tx se reduce de 1000 a 512 entradas. Wide-LLQ está activado de forma predeterminada para todos los tipos de instancias de Nitro v4 y posteriores.

  - Los tipos de instancias de Nitro v4 tienen un tamaño de anillo Tx Wide-LLQ máximo predeterminado de 512 entradas, que no se puede cambiar.
  - Los tipos de instancias de Nitro v5 tienen un tamaño de anillo Tx Wide-LLQ predeterminado de 512 entradas, que puede aumentar hasta 1000 entradas.

Puede ejecutar los siguientes comandos ethtool para ajustar el tamaño de LLQ. Para obtener más información sobre cómo controlar, consultar y habilitar Wide-LLQ, consulte el tema Large Low-Latency Queue (Large LLQ) del controlador del kernel de Linux para la documentación ENA en el repositorio de GitHub de Amazon Drivers.

Encuentre la profundidad máxima para sus colas de Tx:

```
ethtool -g interface
```

Defina sus colas de Tx a la profundidad máxima:

```
ethtool -G interface tx depth
```

Solución de problemas del controlador Elastic Network Adapter para Windows

El Elastic Network Adapter (ENA) está diseñado para mejorar el estado del sistema operativo y reducir el comportamiento inesperado del hardware o los errores que pueden interrumpir el funcionamiento de su instancia de Windows. La arquitectura ENA mantiene los errores de la unidad o el dispositivo lo más transparente posible para el sistema operativo.

Instalación del controlador Elastic Network Adapter (ENA)

Si su instancia no está basada en una de las imágenes de máquina de Amazon (AMI) de Windows más recientes que ofrece Amazon, utilice el siguiente procedimiento para instalar el controlador ENA actual en su instancia. Debería realizar esta actualización cuando sea adecuado reiniciar la instancia. Si el script de instalación no reinicia automáticamente la instancia, le recomendamos que la reinicie como paso final.

Si utiliza un volumen de almacén de instancias para almacenar datos mientras la instancia está en ejecución, esos datos se borran al detener la instancia. Antes de detener su instancia, compruebe que ha copiado los datos que necesita de los volúmenes de almacén de instancias al almacenamiento persistente, como Amazon EBS o Amazon S3.

Requisitos previos

Para instalar o actualizar el controlador ENA, la instancia de Windows debe cumplir los siguientes requisitos previos:

- Tener PowerShell versión 3.0 o posterior instalado

Paso 1: realice copias de seguridad de los datos

Le recomendamos crear una AMI de copia de seguridad, en caso de que no pueda revertir los cambios a través del Administrador de dispositivos. Para crear una AMI de respaldo con la AWS Management Console, siga estos pasos:

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Seleccione la instancia que requiere la actualización del controlador, seleccione Detener instancia en el menú Estado de la instancia.
4. Una vez que la instancia se haya detenido, vuelva a seleccionarla. Para crear la copia de seguridad, seleccione Imagen y plantillas en el menú Acciones y, a continuación, elija Crear imagen.
5. Para reiniciar la instancia, seleccione Iniciar instancia en el menú Estado de la instancia.

Paso 2: instale o actualice el controlador ENA

Puede instalar o actualizar el controlador ENA con Distributor AWS Systems Manager o con los cmdlets de PowerShell. Para obtener más instrucciones, seleccione la pestaña correspondiente al método que desea utilizar.

Systems Manager Distributor

Puede utilizar la función Systems Manager Distributor para implementar paquetes en los nodos administrados de Systems Manager. Con Systems Manager Distributor, puede instalar el paquete ENA de controladores ENA una vez, o con actualizaciones programadas. Para obtener más información sobre cómo instalar el paquete de controladores ENA (`AwsEnaNetworkDriver`) con Systems Manager Distributor, consulte Instalación o actualización de paquetes en la Guía del usuario de AWS Systems Manager.

PowerShell

En esta sección, se explica cómo descargar e instalar los paquetes de controladores ENA en la instancia con los cmdlets de PowerShell.

Opción 1: Descargar y extraer la versión más reciente

1. Conéctese a la instancia e inicie sesión como administrador local.
2. Utilice el cmdlet de invoke-webrequest para descargar el paquete de controladores más reciente:

```
PS C:\> invoke-webrequest https://ec2-windows-drivers-
downloads.s3.amazonaws.com/ENA/Latest/AwsEnaNetworkDriver.zip -
outfile $env:USERPROFILE\AwsEnaNetworkDriver.zip
```

> **Note**
>
> Si recibe un error al descargar el archivo y está usando Windows Server 2016 o una versión anterior, es posible que sea necesario habilitar TLS 1.2 para su terminal PowerShell. Puede habilitar TLS 1.2 para la sesión actual de PowerShell con el siguiente comando y luego volver a intentarlo:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol =
>  [Net.SecurityProtocolType]::Tls12
> ```
>
> Como alternativa, puede descargar el paquete de controladores más reciente desde una ventana del navegador de su instancia.

3. Use el cmdlet de expand-archive para extraer el archivo zip que descargó en su instancia:

```
PS C:\> expand-archive $env:userprofile\AwsEnaNetworkDriver.zip -
DestinationPath $env:userprofile\AwsEnaNetworkDriver
```

Opción 2: Descargar y extraer una versión específica

1. Conéctese a la instancia e inicie sesión como administrador local.
2. Descargue el paquete de controladores ENA para la versión específica que desee desde el enlace de versión de la tabla Controlador de ENA de Windows.

3. Extraiga el archivo zip a la instancia.

Instale el controlador ENA con PowerShell

Los pasos de instalación son los mismos tanto si descargó el controlador más reciente como una versión específica. Para instalar el controlador ENA, siga estos pasos.

1. Para instalar el controlador, ejecute el script de PowerShell `install.ps1` desde el directorio `AwsEnaNetworkDriver` en su instancia. Si aparece un error, asegúrese de que está utilizando PowerShell 3.0 o posterior.
2. Si el instalador no reinicia automáticamente la instancia, ejecute el cmdlet de PowerShell Restart-Computer.

```
PS C:\> Restart-Computer
```

Paso 3 (opcional): verifique la versión del controlador ENA después de la instalación

Para asegurarse de que el paquete de controladores ENA se ha instalado correctamente en la instancia, puede comprobar la nueva versión de la siguiente manera:

1. Conéctese a la instancia e inicie sesión como administrador local.
2. Para abrir el administrador de dispositivos de Windows, ingrese `devmgmt.msc` en el cuadro Ejecutar.
3. Seleccione Aceptar. Se abre la ventana del administrador de dispositivos.
4. Seleccione la flecha a la izquierda de Adaptadores de red para ampliar la lista.
5. Elija el nombre o abra el menú de contexto de Amazon Elastic Network Adapter y luego seleccione Propiedades. Se abre el cuadro de diálogo Propiedades del adaptador de red elástico de Amazon.

> **Note**
>
> Todos los adaptadores ENA utilizan el mismo controlador. Si tiene varios adaptadores ENA, puede seleccionar cualquiera de ellos para actualizar el controlador de todos los adaptadores ENA.

6. Para comprobar la versión actual que está instalada, abra la pestaña Controlador y compruebe la Versión del controlador. Si la versión actual no coincide con la versión de destino, consulte Solución de problemas del controlador Elastic Network Adapter para Windows.

Revertir la instalación de un controlador ENA

Si hay algún problema con la instalación, puede que tenga que revertir el controlador. Siga estos pasos para volver a la versión anterior del controlador ENA que estaba instalado en la instancia.

1. Conéctese a la instancia e inicie sesión como administrador local.
2. Para abrir el administrador de dispositivos de Windows, ingrese `devmgmt.msc` en el cuadro Ejecutar.
3. Seleccione Aceptar. Se abre la ventana del administrador de dispositivos.
4. Seleccione la flecha a la izquierda de Adaptadores de red para ampliar la lista.
5. Elija el nombre o abra el menú de contexto de Amazon Elastic Network Adapter y luego seleccione Propiedades. Se abre el cuadro de diálogo Propiedades del adaptador de red elástico de Amazon.

> **Note**
>
> Todos los adaptadores ENA utilizan el mismo controlador. Si tiene varios adaptadores ENA, puede seleccionar cualquiera de ellos para actualizar el controlador de todos los adaptadores ENA.

6. Para revertir el controlador, abra la pestaña Controlador y seleccione Revertir controlador. Esto abre la ventana Reversión del paquete de controladores.

> **Note**
>
> Si la pestaña Controlador no muestra la acción Revertir el controlador o si la acción no está disponible, significa que el Almacén de controladores de la instancia no contiene el paquete de controladores instalado anteriormente. Para solucionar este problema, consulte Escenarios de solución de problemas y amplíe la sección Versión inesperada del controlador ENA instalado. Para obtener más información sobre el proceso de selección de paquetes de controladores de dispositivos, consulte Cómo

selecciona Windows un paquete de controladores para un dispositivo en el sitio web de documentación de Microsoft.

Recopilar información de diagnóstico de la instancia

Los pasos para abrir las herramientas del sistema operativo (SO) Windows varían según la versión del SO instalada en la instancia. En las siguientes secciones, utilizamos el diálogo Ejecutar para abrir las herramientas, que funciona igual en todas las versiones del sistema operativo. Sin embargo, puede acceder a estas herramientas utilizando el método que prefiera.

Acceso al cuadro de diálogo Ejecutar

- Uso de la combinación de teclas del logotipo de Windows: `Windows` + `R`
- Utilizar la barra de búsqueda:
  - Escriba `run` en la barra de búsqueda.
  - Seleccione la aplicación Ejecutar de los resultados de la búsqueda.

Algunos pasos requieren el menú de contexto para acceder a las propiedades o acciones sensibles al contexto. Hay varias formas de hacerlo, según su versión y el hardware de su sistema operativo.

Accede al menú de contexto

- Con el ratón: haga clic con el botón derecho en un elemento para abrir su menú de contexto.
- Uso del teclado:
  - En función de la versión del sistema operativo, utilice `Shift` + `F10`, o bien `Ctrl` + `Shift` + `F10`.
  - Si tiene la tecla de contexto en el teclado (tres líneas horizontales en un cuadro), seleccione el elemento que desee y, a continuación, presione la tecla de contexto.

Si puede conectarse a su instancia, utilice las siguientes técnicas para recopilar información de diagnóstico para solucionar problemas.

Verificar el estado del dispositivo ENA

Para verificar el estado del controlador de Windows ENA mediante el administrador de dispositivos de Windows, siga estos pasos:

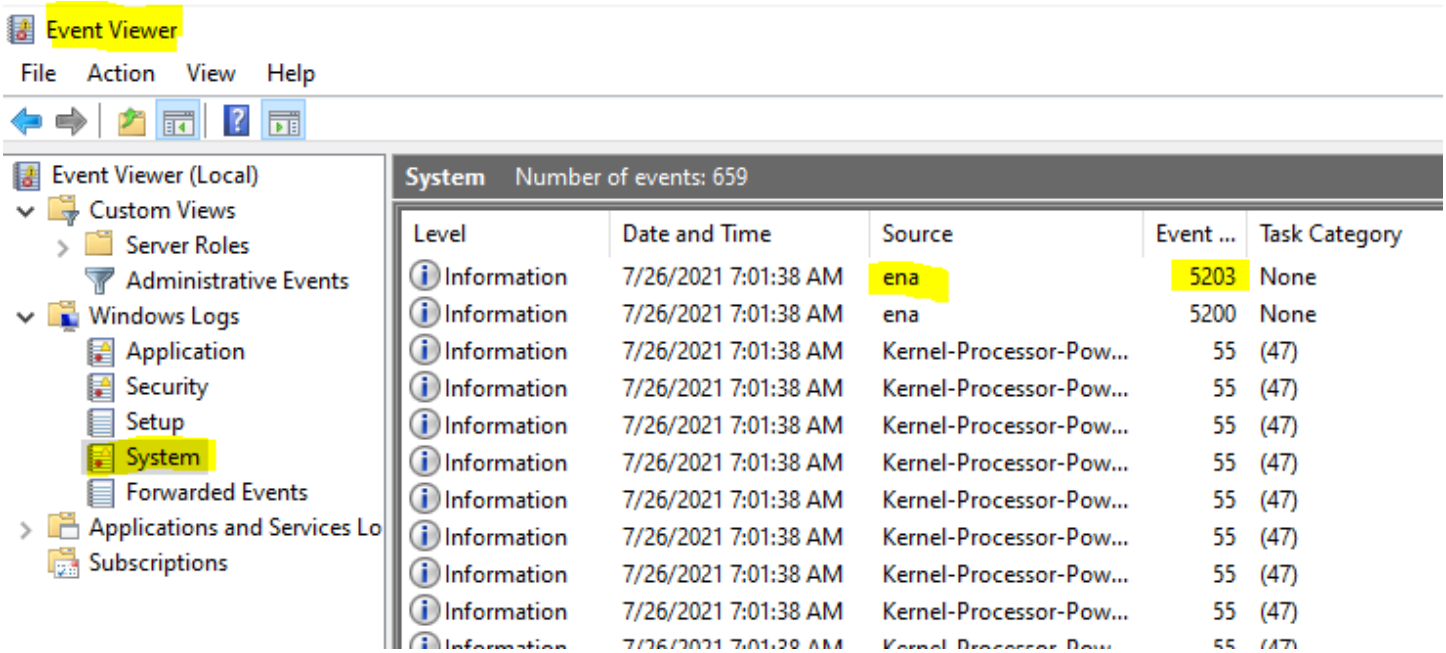
1. Abra el icono Ejecutar mediante alguno de los métodos descritos en la sección anterior.
2. Para abrir el administrador de dispositivos de Windows, ingrese `devmgmt.msc` en el cuadro Run (Ejecutar).
3. Seleccione Aceptar. Se abre la ventana del administrador de dispositivos.
4. Seleccione la flecha a la izquierda de Adaptadores de red para ampliar la lista.
5. Elija el nombre o abra el menú de contexto de Amazon Elastic Network Adapter y luego seleccione Propiedades. Se abre el cuadro de diálogo Propiedades del adaptador de red elástico de Amazon.
6. Compruebe que el mensaje de la pestaña General diga “Este dispositivo funciona correctamente”.

Investigar mensajes de eventos del controlador

Para revisar los registros de eventos del controlador de Windows ENA mediante el lector de eventos de Windows, siga estos pasos:

1. Abra el icono Run (Ejecutar) mediante alguno de los métodos descritos en la sección anterior.
2. Para abrir el lector de eventos de Windows, ingrese `eventvwr.msc` en el cuadro Ejecutar.
3. Seleccione Aceptar. Se abrirá la ventana del lector de eventos.
4. Amplíe el menú Registros de Windows y, a continuación, elija Sistema.
5. En Acciones, en el panel superior derecho, elija Filtrar registro actual. Se muestra el cuadro de diálogo de filtrado.
6. En el cuadro Orígenes de eventos, ingrese `ena`. Esto limita los resultados a los eventos generados por el controlador de Windows ENA.
7. Seleccione Aceptar. Muestra los resultados del registro de eventos filtrados en las secciones de detalles de la ventana.
8. Para obtener más detalles, seleccione un mensaje de evento de la lista.

En el siguiente ejemplo, se muestra un evento de controlador ENA en la lista de eventos del sistema del lector de eventos de Windows:



Resumen de mensajes de evento

En la tabla siguiente, se muestran los mensajes de eventos que genera el controlador de Windows ENA.

Entrada

ID de evento	Descripción del evento del controlador ENA	Tipo
5001	El hardware no tiene recursos	Error
5002	El adaptador ha detectado un error de hardware	Error
5005	Se ha agotado el tiempo de espera del adaptador en el funcionamiento del NDIS que no se completó oportunam ente	Error
5032	El adaptador no ha podido restablecer el dispositivo	Error

ID de evento	Descripción del evento del controlador ENA	Tipo
5200	Se ha inicializado el adaptador	Informativo
5201	Se ha detenido el adaptador	Informativo
5202	Se ha pausado el adaptador	Informativo
5203	Se ha reiniciado el adaptador	Informativo
5204	El adaptador se ha apagado	Informativo
5205	Se ha restablecido el adaptador	Error
5206	El adaptador ha sido eliminado sorpresivamente	Error
5208	Error en la rutina de inicializ ación del adaptador	Error
5210	El adaptador ha encontrado y recuperado correctamente un problema interno	Error

Revisar las métricas de rendimiento

El controlador ENA de Windows publica métricas de rendimiento de la red desde las instancias en las que están habilitadas. Puede ver y habilitar métricas en la instancia mediante la aplicación nativa Performance Monitor (Monitor de rendimiento). Para obtener más información acerca de las métricas que produce el controlador ENA para Windows, consulte Monitoreo del rendimiento de la red de la instancia de EC2.

En los casos en que las métricas de ENA están habilitadas y el agente de Amazon CloudWatch está instalado, CloudWatch recopila las métricas asociadas a los contadores del Monitor de rendimiento de Windows, así como algunas métricas avanzadas para ENA. Estas métricas se recopilan además de las métricas habilitadas de forma predeterminada en las instancias de EC2. Para obtener más

información acerca de las métricas, consulte Métricas recopiladas por el agente de CloudWatch en la Guía del usuario de Amazon CloudWatch.

> **Note**
>
> Las métricas de rendimiento están disponibles para las versiones 2.4.0 y posteriores del controlador de ENA (también para la versión 2.2.3). La versión 2.2.4 del controlador de ENA se revirtió debido a la posible disminución del rendimiento en las instancias de EC2 de sexta generación. Le recomendamos que actualice a la versión actual del controlador para asegurarse de tener las últimas actualizaciones.

Algunas de las formas en las que puede utilizar las métricas de rendimiento incluyen:

- Solucione problemas de rendimiento de instancias.
- Elija el tamaño de instancia adecuado para una carga de trabajo.
- Planifique de forma proactiva las actividades de escalado.
- Aplicaciones de referencia para determinar si maximizan el rendimiento disponible en una instancia.

Frecuencia de actualización

De forma predeterminada, el controlador actualiza las métricas mediante un intervalo de 1 segundo. Sin embargo, la aplicación que recupera las métricas podría utilizar un intervalo diferente para las encuestas. Puede cambiar el intervalo de actualización en el Administrador de dispositivos mediante las propiedades avanzadas del controlador.

Para cambiar el intervalo de actualización de métricas del controlador de Windows ENA, siga estos pasos:

1. Abra el icono Run (Ejecutar) mediante alguno de los métodos descritos en la sección anterior.
2. Para abrir el administrador de dispositivos de Windows, ingrese `devmgmt.msc` en el cuadro Run (Ejecutar).
3. Seleccione Aceptar. Se abre la ventana del administrador de dispositivos.
4. Seleccione la flecha a la izquierda de Adaptadores de red para ampliar la lista.

5. Elija el nombre o abra el menú de contexto de Amazon Elastic Network Adapter y luego seleccione Propiedades. Se abre el cuadro de diálogo Propiedades del adaptador de red elástico de Amazon.
6. Abra la pestaña Avanzado en la ventana emergente.
7. Desde la lista Propiedades, elija Intervalo de actualización de métricas para cambiar el valor.
8. Elija Aceptar cuando haya terminado.

Restablecimiento del adaptador ENA

El proceso de restablecimiento se inicia cuando el controlador de Windows ENA detecta un error en un adaptador y marca el adaptador como incorrecto. El controlador no puede restablecerse por sí mismo, por lo que depende del sistema operativo para verificar el estado del adaptador y llamar al identificador de restablecimiento del controlador de Windows ENA. El proceso de restablecimiento podría dar lugar a un breve periodo en el que se produce una pérdida de tráfico. Sin embargo, las conexiones TCP deberían poder recuperarse.

El adaptador ENA también puede solicitar indirectamente un procedimiento de restablecimiento del dispositivo, al no enviar una notificación de mantenimiento. Por ejemplo, si el adaptador ENA llega a un estado desconocido después de cargar una configuración irrecuperable, podría dejar de enviar notificaciones persistentes.

Causas comunes para restablecer el adaptador ENA

- Faltan mensajes persistentes

  El adaptador ENA publica eventos persistentes a intervalos establecidos (por lo general una vez por segundo). El controlador de Windows ENA implementa un mecanismo watchdog para verificar periódicamente la presencia de estos mensajes persistentes. Si detecta uno o más mensajes nuevos desde la última vez que lo verificó, registra un resultado satisfactorio. De lo contrario, el controlador concluye que el dispositivo ha sufrido un error e inicia una secuencia de restablecimiento.
- Los paquetes están atascados en las colas de transmisión

  El adaptador ENA verifica que los paquetes fluyan a través de las colas de transmisión según lo esperado. El controlador de Windows ENA detecta si los paquetes se atascan e inicia una secuencia de restablecimiento si esto sucede.
- Tiempo de espera de lectura para los registros de E/S asignadas para memoria (MMIO)

A fin de limitar las operaciones de lectura de E/S asignadas para memoria (MMIO), el controlador de Windows ENA accede a los registros MMIO solo durante los procesos de inicialización y restablecimiento. Si el controlador detecta un tiempo de espera, se lleva a cabo una de las siguientes acciones, según el proceso que se esté ejecutando:

- Si se detecta un tiempo de espera durante la inicialización, el flujo falla, lo que hace que el controlador muestre un signo de exclamación amarillo junto al adaptador ENA en el Administrador de dispositivos de Windows.
- Si se detecta un tiempo de espera durante el restablecimiento, el flujo falla. A continuación, el sistema operativo inicia una eliminación sorpresa del adaptador ENA y lo recupera al detener e iniciar el adaptador que se eliminó. Para obtener más información sobre la eliminación sorpresa de una tarjeta de interfaz de red (NIC), consulte Manejo de la eliminación sorpresa de una NIC en la documentación para el Desarrollador de hardware de Microsoft Windows.

Escenarios de solución de problemas

Los siguientes escenarios pueden ayudarlo a solucionar problemas que pudieran surgir con el controlador de Windows ENA. Le recomendamos que comience con la actualización del controlador ENA, si no tiene la última versión. Para encontrar el controlador más reciente para la versión del sistema operativo Windows, consulte Controlador de ENA de Windows.

Versión inesperada del controlador ENA instalado

Descripción

Tras seguir los pasos para instalar una versión específica del controlador ENA, el Administrador de dispositivos de Windows muestra que Windows ha instalado una versión diferente del controlador ENA.

Causa

Al ejecutar la instalación de un paquete de controladores, Windows clasifica todos los paquetes de controladores válidos para el dispositivo determinado en el almacén de controladores local antes de que comience. A continuación, seleccione el paquete con el valor de clasificación más bajo como el que mejor coincide. Puede ser diferente del paquete que pretendía instalar. Para obtener más información sobre el proceso de selección de paquetes de controladores de dispositivos, consulte Cómo selecciona Windows un paquete de controladores para un dispositivo en el sitio web de documentación de Microsoft.

Solución

Para asegurarse de que Windows instale la versión del paquete de controladores que haya elegido, puede eliminar los paquetes de controladores de menor rango de la Tienda de controladores con la herramienta de línea de comandos PNPUtil.

Para actualizar el controlador ENA, siga estos pasos:

1. Conéctese a la instancia e inicie sesión como administrador local.
2. Abra la ventana de propiedades del Administrador de dispositivos, tal como se describe en la sección Verificar el estado del dispositivo ENA. Se abre la pestaña General de la ventana Propiedades del adaptador de red elástico de Amazon.
3. Abra la pestaña Controlador.
4. Elija Actualizar controlador. Se abre el cuadro de diálogo Actualizar el software del controlador: adaptador de red elástico de Amazon.
   a. En la página ¿Cómo desea buscar el software de controlador?, elija Buscar software de controlador en el equipo.
   b. En la página Buscar el software del controlador en su ordenador, seleccione Déjame elegir de la lista de controladores de dispositivos de mi equipo, que se encuentra debajo de la barra de búsqueda.
   c. En la página Seleccionar el controlador de dispositivo que desea instalar para este equipo, elija Tener disco....
   d. En la ventana Instalar desde disco, seleccione Examinar... , junto a la ubicación del archivo en el menú desplegable.
   e. Navegue hasta la ubicación en la que descargó el paquete de controladores ENA de destino. Seleccione el archivo nombrado `ena.inf` y elija Abrir.
   f. Para iniciar la instalación, seleccione Aceptar y, a continuación, seleccione Siguiente.
5. Si el instalador no reinicia automáticamente la instancia, ejecute el cmdlet de PowerShell Restart-Computer.

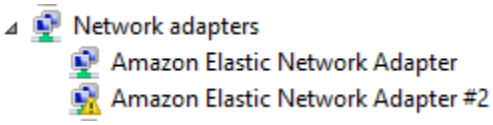
```
PS C:\> Restart-Computer
```

Advertencia de dispositivo para el controlador ENA

Descripción

El icono del adaptador ENA en la sección Adaptadores de red del Administrador de dispositivos muestra un signo de advertencia (un triángulo amarillo con un signo de exclamación en su interior).

En el siguiente ejemplo, se muestra un adaptador ENA con el icono de advertencia del Administrador de dispositivos de Windows:



Causa

Esta advertencia de dispositivo suele deberse a problemas de entorno, que pueden requerir más investigación y, a menudo, requerir un proceso de eliminación para determinar la causa subyacente. Para obtener una lista completa de los errores de dispositivos, consulte Mensajes de error del Administrador en la documentación del Desarrollador de hardware de Microsoft Windows.

Solución

La solución para la advertencia de este dispositivo depende de la causa raíz. El proceso de eliminación descrito aquí incluye algunos pasos básicos para ayudar a identificar y resolver los problemas más comunes que podrían tener una solución sencilla. Se requiere un análisis de causa raíz adicional cuando estos pasos no resuelven el problema.

Siga estos pasos para ayudar a identificar y resolver problemas comunes:

1. Detener e iniciar el dispositivo

   Abra la ventana de propiedades del Administrador de dispositivos, tal como se describe en la sección Verificar el estado del dispositivo ENA. Se abre la pestaña General de la ventana Propiedades de Amazon Elastic Network Adapter, donde Estado del dispositivo muestra el código de error y un mensaje breve.

   a. Abra la pestaña Driver (Controlador).

   b. Elija Desactivar dispositivo y responda Sí al mensaje de advertencia que aparecerá.

   c. Elija Habilitar dispositivo.

2. Detenga e inicie la instancia de EC2

   Si el adaptador sigue mostrando el icono de advertencia en el Administrador de dispositivos, el siguiente paso es detener e iniciar la instancia de EC2. Esto vuelve a iniciar la instancia en un hardware diferente en la mayoría de los casos.
3. Investigar el posible problema de los recursos de instancia

   Si ha detenido e iniciado la instancia de EC2 y el problema continúa, esto podría indicar un problema de recursos en la instancia, como memoria insuficiente.

Tiempo de espera de conexión con el restablecimiento del adaptador (códigos de error 5007, 5205)

Descripción

El lector de eventos Windows muestra el tiempo de espera del adaptador y los eventos de restablecimiento que se producen en conjunto para los adaptadores ENA. Los mensajes se parecen a los siguientes ejemplos:

- ID de evento 5007: Amazon Elastic Network Adapter: se ha agotado el tiempo de espera durante una operación.
- ID de evento 5205: Amazon Elastic Network Adapter: se ha iniciado el restablecimiento del adaptador.

Reestablecer el adaptador provoca una interrupción mínima del tráfico. Incluso cuando haya varios reinicios, sería inusual que provocaran cualquier interrupción grave de la red.

Causa

Esta secuencia de eventos indica que el controlador de Windows ENA inició un restablecimiento de un adaptador ENA que no respondía. Sin embargo, el mecanismo que utiliza el controlador de dispositivo para detectar este problema está sujeto a falsos positivos como resultado de la falta de CPU 0.

Solución

Si esta combinación de errores se produce con frecuencia, verifique las asignaciones de recursos para ver dónde pueden resultar útiles hacer ajustes.

1. Abra el icono Run (Ejecutar) mediante alguno de los métodos descritos en la sección anterior.

2. Para abrir el Monitor de recursos de Windows, ingrese `resmon` en el cuadro Ejecutar.
3. Seleccione Aceptar. Se abre la ventana del Monitor de recursos.
4. Abra la pestaña CPU. Los gráficos de uso por CPU se muestran en el lado derecho de la ventana del Monitor de recursos.
5. Verifique los niveles de uso de la CPU 0 para ver si son demasiado altos.

Recomendamos configurar RSS a fin de excluir la CPU 0 para el adaptador ENA en tipos de instancias más grandes (más de 16 vCPU). Para los tipos de instancias más pequeños, la configuración de RSS podría mejorar la experiencia. Sin embargo, dado que hay menos núcleos disponibles, es necesario realizar pruebas para garantizar que la restricción de los núcleos de CPU no afecte negativamente al rendimiento.

Utilice el comando Set-NetAdapterRss a fin de configurar RSS para el adaptador ENA, tal y como se muestra en el ejemplo siguiente.

```
Set-NetAdapterRss -name (Get-NetAdapter | Where-Object {$_.InterfaceDescription -like
 "*Elastic*"}).Name -Baseprocessorgroup 0 -BaseProcessorNumber 1
```

La migración a una infraestructura de instancias de sexta generación afecta al rendimiento o la conexión

Descripción

Si migra a una instancia de EC2 de sexta generación, es posible que experimente una reducción en el rendimiento o errores en los datos adjuntos de ENA si no ha actualizado la versión del controlador de Windows ENA.

Causa

Los tipos de instancias de EC2 de sexta generación requieren la siguiente versión mínima del controlador de ENA para Windows, según el sistema operativo (SO) de la instancia.

Versión mínima

Versión de Windows Server	Versión del controlador ENA
Windows Server 2008 R2	2.2.3 o 2.4.0

Versión de Windows Server	Versión del controlador ENA
Windows Server 2012 y versiones posteriores	2.2.3 y versiones posteriores
Estación de trabajo Windows	2.2.3 y versiones posteriores

Solución

Antes de actualizar a una instancia de EC2 de sexta generación, asegúrese de que la AMI desde la que inicie tenga controladores compatibles según el SO de la instancia, como se muestra en la tabla anterior. Para obtener más información, consulte ¿Qué debo hacer antes de migrar mi instancia de EC2 a una instancia de sexta generación para asegurarme de obtener el máximo rendimiento de la red? en el Centro de conocimiento de AWS re:Post.

Rendimiento inferior al óptimo de la interfaz de red elástica

Descripción

La interfaz ENA no tiene el rendimiento esperado.

Causa

El análisis de causa raíz de los problemas de rendimiento es un proceso de eliminación. Hay demasiadas variables involucradas para identificar una causa común.

Solución

El primer paso del análisis de causa raíz es revisar la información de diagnóstico de la instancia que no funciona según lo esperado, con el fin de determinar si hay errores que podrían estar causando el problema. Para obtener más información, consulte la sección Recopilar información de diagnóstico de la instancia.

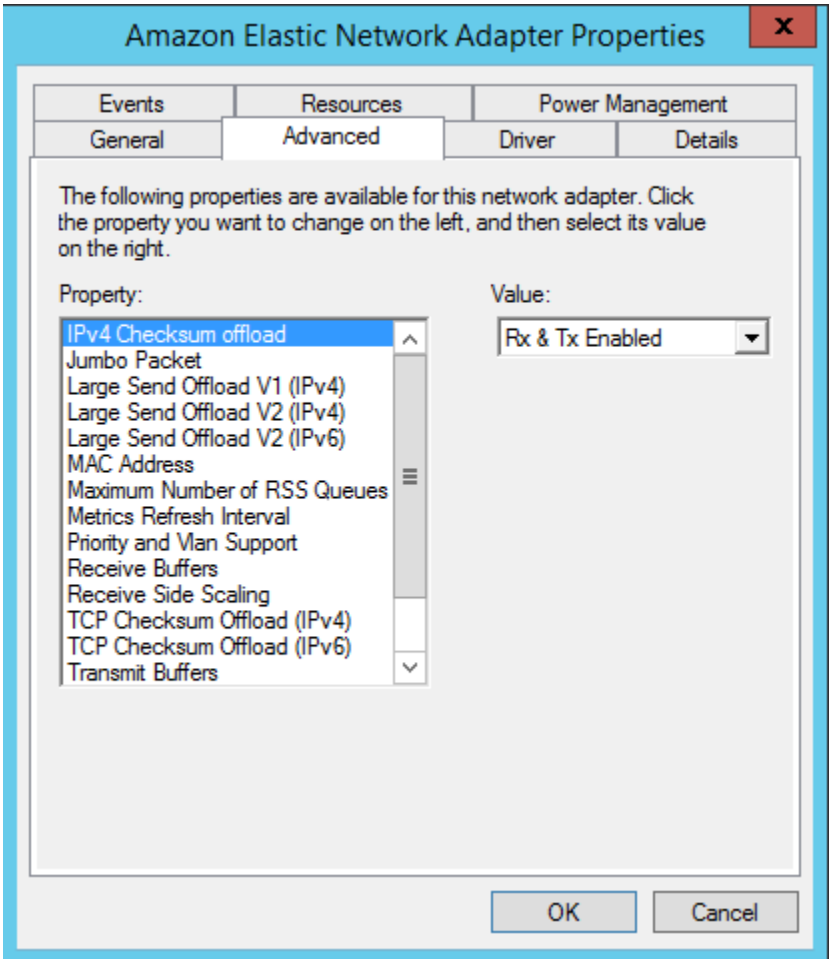
Para conseguir el máximo rendimiento de red en instancias con redes mejoradas, es posible que necesite modificar la configuración predeterminada del sistema operativo. Otras optimizaciones (como activar la descarga de la suma de comprobación y habilitar RSS, por ejemplo) ya están en marcha en las AMI oficiales de Windows de forma predeterminada. Para obtener otras optimizaciones que puede aplicar al adaptador ENA, consulte los ajustes de rendimiento que se muestran en Ajustes de rendimiento del adaptador ENA.

Le recomendamos que proceda con precaución y limite los ajustes de propiedades del dispositivo a los que se enumeran en esta sección, o a los cambios específicos recomendados por el equipo de soporte de AWS.

Para cambiar las propiedades del adaptador ENA, siga estos pasos:

1. Abra el icono Run (Ejecutar) mediante alguno de los métodos descritos en la sección anterior.
2. Para abrir el administrador de dispositivos de Windows, ingrese `devmgmt.msc` en el cuadro Run (Ejecutar).
3. Seleccione Aceptar. Se abre la ventana del administrador de dispositivos.
4. Seleccione la flecha a la izquierda de Adaptadores de red para ampliar la lista.
5. Elija el nombre o abra el menú de contexto de Amazon Elastic Network Adapter y luego seleccione Propiedades. Se abre el cuadro de diálogo Propiedades del adaptador de red elástico de Amazon.
6. Para realizar los cambios, abra la pestaña Avanzado.
7. Cuando haya terminado, elija Aceptar para guardar los cambios.

El siguiente ejemplo, se muestra una propiedad del adaptador ENA en el Administrador de dispositivo de Windows:



Ajustes de rendimiento del adaptador ENA

La tabla siguiente incluye propiedades que se pueden ajustar para mejorar el rendimiento de la interfaz ENA.

Entrada

Propiedad	Descripción	Valor predeterminado	Ajuste
Búferes de recepción	Controla el número de entradas de las colas de recepción de software.	1024	Se puede aumentar hasta un máximo de 8192.
Escala lateral de recepción (RSS)	Permite la distribuc ión eficiente del	Habilitado	Puede distribuir la carga entre varios

Propiedad	Descripción	Valor predeterminado	Ajuste
	procesamiento de recepción de red en varias CPU de sistemas multiprocesador.		procesadores. Para obtener más información, consulte Optimización del rendimiento de la red en instancias de Windows.

Propiedad	Descripción	Valor predeterminado	Ajuste
Número máximo de colas RSS	Establece el número máximo de colas RSS permitidas cuando RSS está habilitado.	32	El número de colas RSS se determina durante la inicializ ación del controlador e incluye las siguiente s limitaciones (entre otras): • Límite de cola RSS establecido por esta propiedad • Límites de instancia s (recuento de vCPU) • Límites de generación de hardware (hasta 8 colas RSS en ENAv1 y hasta 32 colas RSS en ENAv2) Puede establecer el valor del 1 al 32, según los límites de generación de hardware y instancia . Para obtener más información, consulte Optimización del

Propiedad	Descripción	Valor predeterminado	Ajuste
			rendimiento de la red en instancias de Windows.
Paquete gigante	Permite el uso de tramas ethernet gigantes (más de 1500 bytes de carga útil).	Deshabilitado (limita la carga útil a 1500 bytes o menos)	El valor se puede configurar en `9015`, que se traduce en 9001 bytes de carga útil. Esta es la carga útil máxima para tramas ethernet gigantes. Consulte Consideraciones para utilizar tramas ethernet gigantes.

Consideraciones para utilizar tramas ethernet gigantes

Las tramas gigantes permiten más de 1500 bytes de datos al aumentar el tamaño de la carga por paquete, lo que aumenta el porcentaje del paquete que no supone una sobrecarga del paquete. De este modo, se necesitan menos paquetes para enviar la misma cantidad de datos utilizables. Sin embargo, el tráfico está limitado a una MTU máxima de 1500 en los siguientes casos:

- Tráfico fuera de una región de AWS determinada para EC2 Classic.
- Tráfico fuera de una única VPC.
- Tráfico a través de un emparejamiento de VPC entre regiones.
- Tráfico a través de conexiones de VPN.
- Tráfico a través de una puerta de enlace de Internet.

> **Note**
>
> Los paquetes de más de 1500 bytes están fragmentados. Si tiene el indicador `Don't Fragment` establecido en el encabezado IP, estos paquetes se eliminan.

Las tramas gigantes se deben utilizar con precaución para el tráfico vinculado a Internet o cualquier tráfico que provenga de una VPC. Los paquetes son fragmentados por sistemas intermedios, lo que ralentiza el tráfico. Para utilizar tramas gigantes dentro de una VPC sin afectar al tráfico saliente que proviene de la VPC, prueba una de las siguientes opciones:

- Configure el tamaño de la MTU por ruta.
- Utilice varias interfaces de red con distintos tamaños de MTU y rutas diferentes.

Casos de uso recomendados para tramas gigantes

Las tramas gigantes pueden ser útiles para el tráfico dentro de las VPC y entre ellas. Recomendamos utilizar tramas gigantes para los siguientes casos de uso:

- En el caso de las instancias que se colocan dentro de un grupo con ubicación en clúster, las tramas gigantes ayudan a obtener el máximo rendimiento de red posible. Para obtener más información, consulte Grupos de ubicación.
- Puede utilizar tramas gigantes para el tráfico entre las VPC y las redes locales a través de AWS Direct Connect. Para obtener más información acerca del uso de AWS Direct Connect y verificar la capacidad de tramas gigantes, consulte Establecer MTU de red para interfaces virtuales privadas o interfaces virtuales de tránsito en la Guía del usuario de AWS Direct Connect.
- Para obtener más información acerca de los tamaños de MTU admitidos para puertas de enlace de tránsito, consulte Cuotas para sus puertas de enlace de tránsito en Puertas de enlace de tránsito de Amazon VPC.

Mejora de la latencia de red para instancias de Amazon EC2 basadas Linux

La latencia de la red es la cantidad de tiempo que tarda un paquete de datos en viajar desde su origen hasta su destino. Las aplicaciones que envían datos a través de la red dependen de las respuestas oportunas para ofrecer una experiencia de usuario positiva. La alta latencia de la red puede provocar varios problemas, como los siguientes:

- Tiempos de carga lentos para páginas web
- Retraso en la transmisión de video
- Problemas para acceder a los recursos en línea

En esta sección se describen los pasos que puede seguir para mejorar la latencia de red en las instancias de Amazon EC2 que se ejecutan en Linux. Para lograr una latencia óptima, siga estos pasos para configurar los ajustes de la instancia, el núcleo y el controlador ENA. Para obtener más información sobre configuración, consulte la Guía de prácticas recomendadas del controlador Linux ENA y optimización del rendimiento en GitHub.

> **Note**
>
> Los pasos y la configuración pueden variar ligeramente según el hardware de red específico, la AMI desde la que lanzó la instancia y el caso de uso de la aplicación. Antes de realizar cualquier cambio, pruebe y supervise minuciosamente el rendimiento de la red para asegurarse de obtener los resultados deseados.

Reduzca los saltos de red

Cada salto que realiza un paquete de datos al moverse de un router a otro aumenta la latencia de la red. Por lo general, el tráfico debe realizar varios saltos para llegar a su destino. Hay dos formas de reducir los saltos de red en sus instancias de Amazon EC2, de la siguiente manera:

- Grupo con ubicación en clúster: al especificar un grupo con ubicación en clúster, Amazon EC2 inicia instancias que se encuentran cerca unas de otras, físicamente dentro de la misma zona de disponibilidad (AZ) con un mayor número de paquetes. La proximidad física de las instancias del grupo les permite aprovechar la conectividad de alta velocidad, lo que se traduce en una latencia baja y un alto rendimiento de flujo único.
- Host dedicado: un host dedicado también es un servidor físico dedicado para su uso. Con un host dedicado, puede iniciar sus instancias para que se ejecuten en el mismo servidor físico. La comunicación entre instancias que se ejecutan en el mismo host dedicado puede realizarse sin saltos adicionales.

Configuración del kernel

La configuración del kernel de Linux puede aumentar o disminuir la latencia de la red. Para lograr sus objetivos de optimización de la latencia, es importante ajustar la configuración del kernel de Linux de acuerdo con los requisitos específicos de su carga de trabajo.

Hay muchas opciones de configuración para el kernel de Linux que pueden ayudar a reducir la latencia de la red. Las opciones más importantes son las siguientes.

- Habilitar el modo de sondeo ocupado: el modo de sondeo ocupado reduce la latencia en la ruta de recepción de la red. Al habilitar el modo de sondeo ocupado, el código de la capa de conexión puede sondear directamente la cola de recepción de un dispositivo de red. La desventaja del sondeo ocupado es el mayor uso de la CPU en el host, que se debe a la búsqueda de nuevos datos en un bucle muy estricto. Hay dos ajustes globales que controlan el número de microsegundos en que se esperan los paquetes de todas las interfaces.

  `busy_read`

  Un tiempo de espera de sondeo ocupado de baja latencia para lecturas de sockets. Controla la cantidad de microsegundos que se esperan a que la capa de sockets lea los paquetes de la cola del dispositivo. Para habilitar la característica de forma global con el comando sysctl, la organización del kernel de Linux recomienda un valor de 50 microsegundos. Para obtener más información, consulte busy_read en la Guía del usuario y del administrador del kernel de Linux.

  ```
  $ C:\> sudo sysctl -w net.core.busy_read=50
  ```

  `busy_poll`

  Un tiempo de espera de sondeo ocupado de baja latencia para sondear y seleccionar. Controla la cantidad de microsegundos que se esperan a que se produzcan eventos. El valor recomendado está comprendido entre 50 y 100 microsegundos, según la cantidad de sockets que esté sondeando. Cuantos más sockets agregue, mayor será el número.

  ```
  $ C:\> sudo sysctl -w net.core.busy_poll=50
  ```

- Configure los estados de suspensión de CPU (estados C): los estados C controlan los niveles de suspensión en los que puede entrar un núcleo cuando está inactivo. Puede que desee controlar los estados C para ajustar el sistema en cuanto a latencia, en lugar del rendimiento. En los estados C más profundos, la CPU está esencialmente “suspendida” y no puede responder a las solicitudes hasta que se active y vuelva a un estado operativo. Hacer que los núcleos pasen al estado de suspensión lleva tiempo y aunque un núcleo en suspensión ofrece más margen para que otro núcleo arranque a una frecuencia superior, el núcleo en suspensión tarda un tiempo en activarse y en funcionar.

  Por ejemplo, si un núcleo al que se asigna que administre un paquete de red interrumpe su suspensión, puede haber un retraso en el servicio que produzca una interrupción. Puede

configurar el sistema para que no utilice estados C más profundos. Sin embargo, si bien esta configuración reduce la latencia de reacción del procesador, también reduce el margen disponible para que otros núcleos alcancen la frecuencia Turbo Boost.

Para reducir la latencia de reacción del procesador, puede limitar los estados C más profundos. Para obtener más información, consulte High performance and low latency by limiting deeper C-states en la Guía del usuario de Amazon Linux 2.

Configuración del controlador ENA

El controlador de red ENA permite la comunicación entre una instancia y una red. El controlador procesa los paquetes de red y los pasa a la pila de red o a la tarjeta Nitro. Cuando entra un paquete de red, la tarjeta Nitro genera una interrupción para que la CPU notifique un evento al software.

Interrumpir

Una interrupción es una señal que un dispositivo o una aplicación envía al procesador. La interrupción indica al procesador que se ha producido un evento o se ha cumplido una condición que requiere atención inmediata. Las interrupciones pueden gestionar tareas urgentes, como recibir datos de una interfaz de red, gestionar eventos de hardware o atender solicitudes de otros dispositivos.

Interrumpir la moderación

La moderación de interrupciones es una técnica que reduce la cantidad de interrupciones que genera un dispositivo al agregarlas o retrasarlas. El propósito de la moderación de interrupciones es mejorar el rendimiento del sistema al reducir la sobrecarga asociada a la gestión de un gran número de interrupciones. Demasiadas interrupciones aumentan el uso de la CPU, lo que afecta negativamente al rendimiento, mientras que muy pocas interrupciones aumentan la latencia.

Moderación dinámica de interrupciones

La moderación dinámica de interrupciones es una forma mejorada de moderación de interrupciones que ajusta dinámicamente la frecuencia de interrupciones en función de la carga del sistema y los patrones de tráfico actuales. Su objetivo es lograr un equilibrio entre reducir la sobrecarga de interrupciones y los paquetes por segundo o ancho de banda.

> **Note**
>
> La moderación dinámica de interrupciones está habilitada de forma predeterminada en algunas AMI (aunque se puede habilitar o deshabilitar en todas las AMI).

Para minimizar la latencia de la red, puede ser necesario deshabililar la moderación de interrupciones. Sin embargo, esto también puede aumentar la sobrecarga del procesamiento de interrupciones. Es importante encontrar el equilibrio adecuado entre reducir la latencia y minimizar los gastos generales. Los comandos `ethtool` pueden ayudarle a configurar la moderación de interrupciones. De forma predeterminada, `rx-usecs` se establece en `20` y `tx-usecs` se establece en 64.

Para obtener la configuración de moderación de interrupciones actual, utilice el siguiente comando.

```
$ C:\> ethtool -c interface | egrep "rx-usecs:|tx-usecs:|Adaptive RX"
Adaptive RX: on  TX: off
rx-usecs: 20
tx-usecs: 64
```

Para deshabilitar la modificación de interrupciones y la moderación dinámica de interrupciones, utilice el siguiente comando.

```
$ C:\> sudo ethtool -C interface adaptive-rx off rx-usecs 0 tx-usecs 0
```

Consideraciones sobre el Nitro System para ajustar el rendimiento

El sistema Nitro es una recopilación de componentes de hardware y software integrados en AWS que permiten alcanzar un alto rendimiento, una gran disponibilidad y mucha seguridad. El sistema Nitro proporciona capacidades de tipo bare metal que eliminan la sobrecarga de la virtualización y admiten cargas de trabajo que requieren acceso completo al hardware del host. Para obtener más información, consulte AWS Nitro System.

Todos los tipos de instancias de EC2 de la generación actual procesan paquetes de red en tarjetas Nitro de EC2. En este tema, se describe la gestión de paquetes de alto nivel en la tarjeta Nitro, los aspectos comunes de la arquitectura y la configuración de la red que afectan al rendimiento de la gestión de paquetes y las medidas que puede tomar para lograr el máximo rendimiento en sus instancias basadas en Nitro.

Las tarjetas Nitro gestionan todas las interfaces de entrada y salida (E/S), como aquellas necesarias para las Virtual Private Clouds (VPC). Para todos los componentes que envían o reciben información a través de la red, las tarjetas Nitro actúan como un dispositivo de computación autónomo para el tráfico de E/S que está físicamente separado de la placa principal del sistema en la que se ejecutan las cargas de trabajo de los clientes.

Flujo de paquetes de red en las tarjetas Nitro

Las instancias de EC2 integradas en el Nitro System tienen capacidades de aceleración de hardware que permiten un procesamiento de paquetes más rápido, medido en función de las tasas de rendimiento de paquetes por segundo (PPS). Cuando una tarjeta Nitro realiza la evaluación inicial de un flujo nuevo, guarda la misma información para todos los paquetes del flujo, como los grupos de seguridad, las listas de control de acceso y las entradas de la tabla de enrutamiento. Cuando procesa paquetes adicionales para el mismo flujo, puede usar la información guardada para reducir la sobrecarga de esos paquetes.

La velocidad de conexión se mide mediante la métrica de conexiones por segundo (CPS). Cada nueva conexión requiere una sobrecarga de procesamiento adicional que debe tenerse en cuenta en las estimaciones de la capacidad de carga de trabajo. Es importante tener en cuenta las métricas de CPS y PPS al diseñar las cargas de trabajo.

Cómo se establece una conexión

Cuando se establece una conexión entre una instancia basada en Nitro y otro punto de conexión, la tarjeta Nitro evalúa el flujo total del primer paquete que se envía o recibe entre los dos puntos de conexión. En el caso de los paquetes subsiguientes del mismo flujo, no suele ser necesaria una reevaluación completa. Sin embargo, hay algunas excepciones. Para obtener más información sobre las excepciones, consulte Paquetes que no utilizan aceleración del hardware.

Las siguientes propiedades definen los dos puntos de conexión y el flujo de paquetes entre ellos. Estas cinco propiedades juntas se conocen como flujo de 5 tuplas.

- IP de origen
- Puerto de origen
- IP de destino
- Puerto de destino
- Protocolo de comunicación

La dirección del flujo de paquetes se conoce como entrada (entrante) y salida (saliente). Las siguientes descripciones de alto nivel resumen el flujo de paquetes de red de extremo a extremo.

- Entrada: cuando una tarjeta Nitro gestiona un paquete de red entrante, lo evalúa comparándolo con las reglas de firewall y las listas de control de acceso vigentes. Realiza un seguimiento de la conexión, la mide y realiza otras acciones, según proceda. A continuación, reenvía el paquete a su destino en la CPU del host.
- Salida: cuando una tarjeta Nitro gestiona un paquete de red saliente, busca el destino de la interfaz remota, evalúa varias funciones de la VPC, aplica límites de velocidad y realiza las demás acciones pertinentes. A continuación, reenvía el paquete a su siguiente destino de salto en la red.

Diseño para un rendimiento óptimo

Para aprovechar las capacidades de rendimiento de su sistema Nitro, debe comprender cuáles son sus necesidades de procesamiento de red y cómo afectan esas necesidades a la carga de trabajo de sus recursos de Nitro. Luego, puede diseñar para lograr un rendimiento óptimo para su entorno de red. La configuración de la infraestructura y el diseño y la configuración de la carga de trabajo de las aplicaciones pueden afectar tanto al procesamiento de paquetes como a las velocidades de conexión. Por ejemplo, si su aplicación tiene una alta tasa de establecimiento de conexiones, como un servicio de DNS, un firewall o un router virtual, tendrá menos oportunidades de aprovechar la aceleración del hardware que solo se produce una vez establecida la conexión.

Puede configurar las aplicaciones y la infraestructura para agilizar las cargas de trabajo y mejorar el rendimiento de la red. Sin embargo, no todos los paquetes cumplen los requisitos para la aceleración. El sistema Nitro utiliza todo el flujo de la red para las nuevas conexiones y para los paquetes que no cumplen los requisitos para la aceleración.

El resto de esta sección se centrará en las consideraciones de diseño de las aplicaciones y la infraestructura para garantizar que los paquetes fluyan dentro de la ruta acelerada en la medida de lo posible.

Consideraciones

Al configurar el tráfico de red para la instancia, hay muchos aspectos que se deben tener en cuenta y que pueden afectar al rendimiento de los PPS. Una vez establecido un flujo, la mayoría de los paquetes que entran o salen con regularidad cumplen los requisitos para la aceleración. Sin embargo, existen excepciones para garantizar que los diseños de infraestructura y los flujos de paquetes sigan cumpliendo con los estándares de protocolo.

Para obtener el mejor rendimiento de su tarjeta Nitro, debe considerar detenidamente las ventajas y desventajas de los siguientes detalles de configuración para su infraestructura y sus aplicaciones.

Consideraciones sobre infraestructura

La configuración de la infraestructura puede afectar al flujo de paquetes y a la eficiencia del procesamiento. La siguiente lista incluye algunas consideraciones importantes.

Configuración de la interfaz de red con asimetría

Los grupos de seguridad utilizan el seguimiento de conexiones para rastrear información sobre el tráfico que fluye hacia y desde la instancia. El enrutamiento asimétrico, en el que el tráfico entra en una instancia a través de una interfaz de red y sale por una interfaz de red diferente, puede reducir el rendimiento máximo que puede alcanzar una instancia si se realiza un seguimiento de los flujos. Para obtener más información sobre el seguimiento de conexiones de grupos de seguridad, las conexiones no rastreadas y las conexiones rastreadas automáticamente, consulte Seguimiento de conexiones de grupos de seguridad.

Controladores de red

Los controladores de red se actualizan y publican periódicamente. Si sus controladores están desactualizados, eso puede afectar significativamente el rendimiento. Mantenga sus controladores actualizados para asegurarse de tener los parches más recientes y poder aprovechar las mejoras de rendimiento, como la característica de ruta acelerada, que solo está disponible para la última generación de controladores. Los controladores anteriores no son compatibles con la característica de ruta acelerada.

Para aprovechar la característica de ruta acelerada, le recomendamos que instale el controlador ENA más reciente en sus instancias.

Instancias de Linux: controlador ENA para Linux 2.2.9 o posterior. Para instalar o actualizar el controlador ENA para Linux desde el repositorio de GitHub de Amazon Drivers, consulte la sección Compilación de controladores del archivo readme.

Instancias de Windows: controlador ENA para Windows 2.0.0 o posterior. Para instalar o actualizar el controlador ENA para Windows, consulte Instalación del controlador Elastic Network Adapter (ENA).

Distancia entre los puntos de conexión

Una conexión entre dos instancias de la misma zona de disponibilidad puede procesar más paquetes por segundo que una conexión entre regiones debido a la creación de ventanas TCP en

la capa de aplicación, lo que determina la cantidad de datos que pueden estar en movimiento en un momento dado. Las distancias largas entre las instancias aumentan la latencia y disminuyen la cantidad de paquetes que los puntos de conexión pueden procesar.

Consideraciones sobre el diseño de la aplicación

Hay aspectos del diseño y la configuración de la aplicación que pueden afectar a la eficiencia del procesamiento. La siguiente lista incluye algunas consideraciones importantes.

Tamaño del paquete

Los paquetes de mayor tamaño pueden aumentar el rendimiento de los datos que una instancia puede enviar y recibir en la red. Los tamaños de paquete más pequeños pueden aumentar la velocidad de procesamiento de los paquetes, pero esto puede reducir el ancho de banda máximo alcanzado cuando la cantidad de paquetes supera los límites de los PPS.

Si el tamaño de un paquete supera la unidad máxima de transmisión (MTU) de un salto de red, un router situado a lo largo de la ruta podría fragmentarlo. Los fragmentos de paquetes resultantes se consideran excepciones y se procesan a la velocidad estándar (no acelerada). Esto puede provocar variaciones en su rendimiento. Amazon EC2 admite tramas gigantes de 9001 bytes, pero no todos los servicios las admiten. Le recomendamos que evalúe su topología al configurar la MTU.

Compensaciones de protocolo

Los protocolos confiables como el TCP tienen más sobrecarga que los protocolos poco confiables como el UDP. La menor sobrecarga y el procesamiento de red simplificado del protocolo de transporte UDP pueden resultar en una tasa de PPS más alta, pero a expensas de una entrega de paquetes confiable. Si la entrega fiable de paquetes no es fundamental para su aplicación, el UDP podría ser una buena opción.

Microrráfaga

La microrráfaga se produce cuando el tráfico supera las asignaciones durante breves períodos de tiempo, en lugar de distribuirse uniformemente. Esto suele ocurrir en una escala de microsegundos.

Por ejemplo, supongamos que tiene una instancia que puede enviar hasta 10 Gbps y que su aplicación envía los 10 Gb completos en medio segundo. Esta microrráfaga supera los límites permitidos durante el primer medio segundo y no deja nada durante el resto del segundo. Aunque

haya enviado 10 Gb en el período de 1 segundo, los límites en el primer medio segundo pueden provocar que los paquetes se pongan en cola o se descarten.

Puede utilizar un programador de red, como Linux Traffic Control, para acelerar el rendimiento y evitar que los paquetes se queden en cola o se pierdan debido a la microráfaga.

Número de flujos

Un flujo único está limitado a 5 Gbps, a menos que esté dentro de un grupo con ubicación en clústeres que admita hasta 10 Gbps, o si utiliza ENA Express, que admite hasta 25 Gbps.

Del mismo modo, una tarjeta Nitro puede procesar más paquetes en varios flujos en lugar de utilizar un solo flujo. Para alcanzar la velocidad máxima de procesamiento de paquetes por instancia, recomendamos al menos 100 flujos en instancias con un ancho de banda agregado de 100 Gbps o superior. A medida que aumentan las capacidades de ancho de banda agregado, también aumenta la cantidad de flujos necesarios para alcanzar las tasas de procesamiento máximas. La evaluación comparativa lo ayudará a determinar qué configuración necesita para alcanzar las velocidades máximas en su red.

Número de colas Elastic Network Adapter (ENA)

De forma predeterminada, la cantidad máxima de colas ENA se asigna a una interfaz de red en función del tamaño y el tipo de la instancia. Reducir el número de colas puede reducir la tasa máxima de PPS que se puede alcanzar. Recomendamos utilizar la asignación de colas predeterminada para obtener el mejor rendimiento.

Para Linux, la interfaz de red está configurada con el máximo de forma predeterminada. Para las aplicaciones basadas en el kit de desarrollo de planos de datos (DPDK), se recomienda configurar el número máximo de colas disponibles.

Sobrecarga del procesamiento de características

Características como Traffic Mirroring y ENA Express pueden aumentar la sobrecarga del procesamiento, lo que puede reducir el rendimiento absoluto del procesamiento de paquetes. Puede limitar el uso de características o deshabilitarlas para aumentar las tasas de procesamiento de paquetes.

Seguimiento de la conexión para mantener el estado

Sus grupos de seguridad utilizan el seguimiento de conexiones para almacenar información sobre el tráfico hacia y desde la instancia. El seguimiento de la conexión aplica reglas a cada flujo individual de tráfico de red para determinar si el tráfico se permite o se deniega. La tarjeta Nitro

utiliza el seguimiento del flujo para mantener el estado del flujo. A medida que se apliquen más reglas de grupos de seguridad, será necesario trabajar más para evaluar el flujo.

> **Note**
>
> No se rastrean todos los flujos de tráfico de la red. Si se configura una regla de grupo de seguridad con Conexiones sin seguimiento, no es necesario realizar ningún trabajo adicional, excepto en el caso de las conexiones, de las que se realiza un seguimiento automático para garantizar un enrutamiento simétrico cuando hay varias rutas de respuesta válidas.

Paquetes que no utilizan aceleración del hardware

No todos los paquetes pueden aprovechar la aceleración del hardware. La gestión de estas excepciones implica una sobrecarga de procesamiento necesaria para garantizar el buen estado de los flujos de la red. Los flujos de red deben cumplir de manera confiable los estándares de protocolo, ajustarse a los cambios en el diseño de la VPC y enrutar los paquetes solo a los destinos permitidos. Sin embargo, la sobrecarga reduce el rendimiento.

Fragmentos de paquetes

Como se menciona en Consideraciones sobre la aplicación, los fragmentos de paquetes que resultan de paquetes que superan la MTU de la red se gestionan como excepciones y no pueden aprovechar la aceleración del hardware.

Conexiones inactivas

Cuando una conexión no tiene actividad durante un tiempo, incluso si no ha alcanzado su límite de tiempo de espera, el sistema puede despriorizarla. Luego, si los datos llegan después de que se haya perdido la prioridad de la conexión, el sistema debe tratarlos como una excepción para poder volver a conectarse.

Para administrar sus conexiones, puede usar los tiempos de espera del seguimiento de conexiones para cerrar las conexiones inactivas. También puede usar losparámetros Keepalive de TCP para mantener abiertas las conexiones inactivas. Para obtener más información, consulte Tiempo de espera de seguimiento de conexiones inactivas.

Mutación en la VPC

Todas las actualizaciones de los grupos de seguridad, las tablas de enrutamiento y las listas de control de acceso deben volver a evaluarse en la ruta de procesamiento para garantizar que las entradas de ruta y las reglas de los grupos de seguridad se sigan aplicando según lo esperado.

Flujos de ICMP

El Protocolo de mensajes de control de Internet (ICMP) es un protocolo de capa de red que los dispositivos de red utilizan para diagnosticar problemas de comunicación en la red. Estos paquetes siempre utilizan el flujo completo.

Maximización del rendimiento de la red en su Nitro system

Antes de tomar cualquier decisión de diseño o ajustar la configuración de red de la instancia, le recomendamos que siga los siguientes pasos para asegurarse de obtener el mejor resultado:

1. Conozca las ventajas y desventajas de las medidas que puede tomar para mejorar el rendimiento mediante una revisión de Consideraciones.

   Para obtener más información sobre las consideraciones y las prácticas recomendadas para la configuración de la instancia, consulte:

   Instancias de Linux: Guía de optimización del rendimiento y prácticas recomendadas del controlador ENA para Linux en el sitio web de GitHub.

   Instancias de Windows: Prácticas recomendadas para configurar interfaces de red.
2. Compare sus cargas de trabajo con el recuento máximo de flujos activos para determinar una línea de base para el rendimiento de su aplicación. Con una línea de base de rendimiento, puede probar las variaciones en la configuración o el diseño de la aplicación para comprender qué consideraciones tendrán el mayor impacto, especialmente si planea escalarlas verticalmente u horizontalmente.

La siguiente lista contiene las acciones que puede realizar para ajustar el rendimiento de los PPS, en función de las necesidades del sistema.

- Reduzca la distancia física entre dos instancias. Si las instancias de envío y recepción se encuentran en la misma zona de disponibilidad o utilizan grupos con ubicación en clústeres, puede

reducir la cantidad de saltos que debe realizar un paquete para viajar de un punto de conexión a otro.

- Utilice Conexiones sin seguimiento.
- Use el protocolo UDP para el tráfico de red.
- En el caso de las instancias de EC2 con un ancho de banda agregado de 100 Gbps o más, distribuya la carga de trabajo entre 100 o más flujos individuales para distribuir el trabajo de manera uniforme en la tarjeta Nitro.

Monitoreo del rendimiento en las instancias de Linux

Puede usar las métricas de Ethtool en las instancias de Linux para monitorear los indicadores de rendimiento de la red de las instancias, como el ancho de banda, la velocidad de paquetes y el seguimiento de la conexión. Para obtener más información, consulte Monitoreo del rendimiento de la red de la instancia de EC2.

Optimización del rendimiento de la red en instancias de Windows

Para conseguir el máximo rendimiento de red en instancias de Windows con redes mejoradas, es posible que necesite modificar la configuración predeterminada del sistema operativo. Recomendamos los siguientes cambios de configuración para aplicaciones que requieren un alto rendimiento de red. Otras optimizaciones (como activar la descarga de suma de comprobación y habilitar RSS, por ejemplo) ya están configuradas en las AMI oficiales de Windows.

> **Note**
>
> La descarga de la chimenea TCP debe deshabilitarse en la mayoría de los casos de uso, y no está disponible a partir de Windows Server 2016.

Además de estas optimizaciones de sistemas operativos, debe también tener en cuenta la unidad de transmisión máxima (MTU) de su tráfico de red, y ajustarla según su carga de trabajo y arquitectura de red. Para obtener más información, consulte Unidad de transmisión máxima (MTU) de red de la instancia de EC2.

AWS suele medir latencias medias de ida y vuelta entre las instancias iniciadas en un grupo de ubicación en clúster de 50 us y latencias de cola de 200 us en el percentil 99,9. Si sus aplicaciones necesitan latencias bajas de forma continuada, le recomendamos que utilice la última versión de los controladores ENA en instancias basadas en Nitro de rendimiento fijo.

Configurar la afinidad de la CPU de RSS

El escalado lateral de recepción (RSS, por sus siglas en inglés) se utiliza para distribuir la carga de la CPU de tráfico de red en varios procesadores. De forma predeterminada, las AMI de Windows oficiales de Amazon se configuran con el RSS habilitado. Las ENI de ENA proporcionan hasta ocho colas de RSS. Al definir la afinidad de la CPU para las colas de RSS, así como para otros procesos del sistema, es posible distribuir la carga de la CPU en sistemas de varios núcleos, permitiendo que se procese más tráfico de red. En tipos de instancia con más de 16 vCPU, le recomendamos utilizar el cmdlet `Set-NetAdapterRSS` de PowerShell, que excluye manualmente el procesador de arranque (procesador lógico 0 y 1 cuando la tecnología Hyper-Threading está habilitada) desde la configuración RSS para todas las ENI, con el fin de evitar la contención con diversos componentes del sistema.

Windows es compatible con la tecnología Hyper-Threading y garantizará que las colas de RSS de un NIC único se coloque siempre en núcleos físicos distintos. Por lo tanto, a menos que esté desactivada la tecnología Hyper-Threading, para evitar completamente un conflicto con otras NIC, propague la configuración de RSS de cada NIC entre una gama de 16 procesadores lógicos. El cmdlet `Set-NetAdapterRss` le permite definir el rango por NIC de procesadores lógicos válidos definiendo los valores de BaseProcessorGroup, BaseProcessorNumber, MaxProcessingGroup, MaxProcessorNumber y NumaNode (opcional). Si no hay suficientes núcleos físicos para eliminar por completo la contención entre NIC, minimice los rangos de solapamiento o reduzca el número de procesadores lógicos en los rangos de ENI en función de la carga de trabajo prevista del ENI (en otras palabras, un ENI de red de administrador de bajo volumen podría no necesitar tantas colas de RSS asignadas). Además, como se ha indicado con anterioridad, diversos componentes deben ejecutarse en la CPU 0 y, por tanto, recomendamos excluirla de todas las configuraciones de RSS cuando se disponga de suficientes vCPU.

Por ejemplo, cuando hay tres ENI en una instancia de 72 vCPU con dos nodos NUMA con tecnología Hyper-Threading habilitada, los comandos siguientes propagan la carga de red entre las dos CPU sin solapamiento e impiden el uso del núcleo 0 por completo.

```
Set-NetAdapterRss -Name NIC1 -BaseProcessorGroup 0 -BaseProcessorNumber 2 -
MaxProcessorNumber 16
Set-NetAdapterRss -Name NIC2 -BaseProcessorGroup 1 -BaseProcessorNumber 0 -
MaxProcessorNumber 14
Set-NetAdapterRss -Name NIC3 -BaseProcessorGroup 1 -BaseProcessorNumber 16 -
MaxProcessorNumber 30
```

Tenga en cuenta que esta configuración es persistente para todos los adaptadores de red. Si una instancia se redimensiona a una con distinto número de CPU virtuales, debe volver a evaluar la configuración de RSS para cada ENI habilitado. La documentación completa de Microsoft para el cmdlet `Set-NetAdapterRss` se puede encontrar en https://docs.microsoft.com/en-us/powershell/module/netadapter/set-netadapterrss.

Nota especial para las cargas de trabajo de SQL: también le recomendamos revisar la configuración de afinidad de subprocesos de E/S junto con la configuración de RSS de ENI para minimizar la contención de E/S y red para las mismas CPU. Consulte affinity mask Server Configuration Option.

Elastic Fabric Adapter

Elastic Fabric Adapter (EFA) es un dispositivo de red que puede adjuntar a su instancia de Amazon EC2 para acelerar las aplicaciones de informática de alto rendimiento (HPC) y de machine learning. Un EFA le permite obtener el rendimiento de la aplicación de un clúster de HPC en las instalaciones, con la escalabilidad, la flexibilidad y la elasticidad que proporciona la nube de AWS.

Los adaptadores elásticos de estructura (EFA) proporcionan una latencia menor y más constante y un rendimiento superior que el transporte TCP que se utiliza tradicionalmente en los sistemas HPC basados en la nube. Mejora el rendimiento de una comunicación entre instancias que es crítico para el escalado de aplicaciones HCP y de machine learning. Está optimizado para trabajar en la infraestructura de red de AWS existente y se puede escalar en función de los requisitos de aplicaciones.

Los EFA se integran con Libfabric 1.7.0 y versiones posteriores, y son compatibles con Open MPI 5 y versiones posteriores, con la actualización 5 de Intel MPI 2019 para las aplicaciones HPC y con Nvidia Collective Communications Library (NCCL) para las aplicaciones de machine learning.

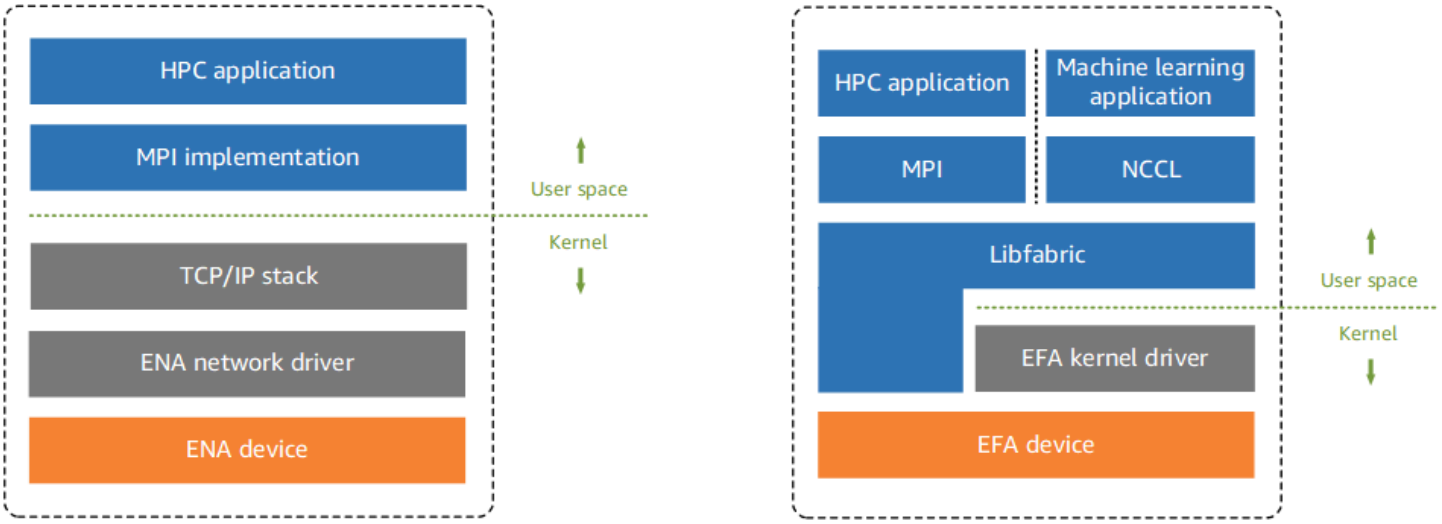
> **Note**
>
> Las capacidades de omisión del sistema operativo de EFAs no son compatibles en las instancias de Windows. Si adjunta un EFA a una instancia de Windows, la instancia funciona como Elastic Network Adapter, sin las capacidades de EFA añadidas.

Contenido

- Interfaces y bibliotecas admitidas
- Tipos de instancias admitidos
- Sistemas operativos compatibles
- Limitaciones de EFA
- Precios de EFA
- Introducción a las instancias P5 y EFA
- Introducción a EFA y MPI
- Introducción a EFA y NCCL
- Trabajar con EFA
- Monitorear un EFA
- Verificar el instalador de EFA mediante una suma de comprobación

Conceptos básicos de EFA

Un EFA es un Elastic Network Adapter (ENA) con capacidades añadidas. Proporciona toda la funcionalidad de un ENA, con funcionalidad adicional de omisión del sistema operativo. La omisión del sistema operativo es un modelo de acceso que permite a las aplicaciones HPC y de machine learning comunicarse directamente con el hardware de interfaz de red para proporcionar una funcionalidad de transporte de confianza y de baja latencia.



Traditional HPC software stack in EC2

HPC software stack in EC2 with EFA

Tradicionalmente, las aplicaciones HPC utilizan Message Passing Interface (MPI) para interaccionar con el transporte de red del sistema. En la nube de AWS, esto ha significado que las aplicaciones

interaccionan con MPI que, a continuación, utiliza la pila TCP/IP del sistema y el controlador de dispositivo de ENA para permitir la comunicación de red entre instancias.

Con un EFA, las aplicaciones HPC utilizan MPI o NCCL para interaccionar con la API de Libfabric. La API Libfabric omite el kernel del sistema operativo y se comunica directamente con el dispositivo EFA para poner paquetes en la red. Esto reduce la sobrecarga y permite que la aplicación HPC se ejecute de forma más eficiente.

> **Note**
>
> Libfabric es un componente principal del marco OpenFabrics Interfaces (OFI), que define y exporta la API de espacio del usuario de OFI. Para obtener más información consulte el sitio web de Libfabric OpenFabrics.

Diferencias entre los EFAs e instancias reservadas

Los Elastic Network Adapters (ENA) proporcionan características de redes de IP tradicionales que son requeridas para admitir las redes de VPC. Los EFA proporcionan las mismas características de redes de IP tradicionales que los ENA y también son compatibles con capacidades de omisión del sistema operativo. La omisión del sistema operativo habilita a las aplicaciones HPC y de machine learning para omitir el kernel del sistema operativo y comunicarse directamente con el dispositivo de EFA.

Interfaces y bibliotecas admitidas

Los EFA admiten las siguientes interfaces y bibliotecas:

- Open MPI 5 y versiones posteriores
- Se prefiere Open MPI 4.0 o una versión más reciente para Graviton
- Intel MPI 2019 Actualización 5 y versiones posteriores
- NVIDIA Collective Communications Library (NCCL) 2.4.2 y posterior

Tipos de instancias admitidos

Los tipos de instancia que se muestran a continuación, admiten EFAs:

- De uso general: m5dn.24xlarge | m5dn.metal | m5n.24xlarge | m5n.metal | m5zn.12xlarge | m5zn.metal | m6a.48xlarge | m6a.metal | m6i.32xlarge | m6i.metal | m6id.32xlarge | m6id.metal | m6idn.32xlarge | m6idn.metal | m6in.32xlarge | m6in.metal | m7a.48xlarge | m7a.metal-48xl | m7g.16xlarge | m7g.metal | m7gd.16xlarge | m7gd.metal | m7i.48xlarge | m7i.metal-48xl
- Optimizadas para la computación: c5n.9xlarge | c5n.18xlarge | c5n.metal | c6a.48xlarge | c6a.metal | c6gn.16xlarge | c6i.32xlarge | c6i.metal | c6id.32xlarge | c6id.metal | c6in.32xlarge | c6in.metal | c7a.48xlarge | c7a.metal-48xl | c7g.16xlarge | c7g.metal | c7gd.16xlarge | c7gd.metal | c7gn.16xlarge | c7gn.metal | c7i.48xlarge | c7i.metal-48xl
- Optimizadas para memoria: r5dn.24xlarge | r5dn.metal | r5n.24xlarge | r5n.metal | r6a.48xlarge | r6a.metal | r6i.32xlarge | r6i.metal | r6idn.32xlarge | r6idn.metal | r6in.32xlarge | r6in.metal | r6id.32xlarge | r6id.metal | r7a.48xlarge | r7a.metal-48xl | r7g.16xlarge | r7g.metal | r7gd.16xlarge | r7gd.metal | r7i.48xlarge | r7i.metal-48xl | r7iz.32xlarge | r7iz.metal-32xl | u7i-12tb.224xlarge | u7in-16tb.224xlarge | u7in-24tb.224xlarge | u7in-32tb.224xlarge | x2idn.32xlarge | x2idn.metal | x2iedn.32xlarge | x2iedn.metal | x2iezn.12xlarge | x2iezn.metal
- Optimizada para almacenamiento: i3en.12xlarge | i3en.24xlarge | i3en.metal | i4g.16xlarge | i4i.32xlarge | i4i.metal | im4gn.16xlarge
- De computación acelerada: dl1.24xlarge | dl2q.24xlarge | g4dn.8xlarge | g4dn.12xlarge | g4dn.16xlarge | g4dn.metal | g5.8xlarge | g5.12xlarge | g5.16xlarge | g5.24xlarge | g5.48xlarge | g6.8xlarge | g6.12xlarge | g6.16xlarge | g6.24xlarge | g6.48xlarge | gr6.8xlarge | inf1.24xlarge | p3dn.24xlarge | p4d.24xlarge | p4de.24xlarge | p5.48xlarge | trn1.32xlarge | trn1n.32xlarge | vt1.24xlarge
- De computación de alto rendimiento: hpc6a.48xlarge | hpc6id.32xlarge | hpc7a.12xlarge | hpc7a.24xlarge | hpc7a.48xlarge | hpc7a.96xlarge | hpc7g.4xlarge | hpc7g.8xlarge | hpc7g.16xlarge

Para ver los tipos de instancias disponibles que son compatibles con los EFA en una región específica

Los tipos de instancia disponibles varían según la región. Para ver los tipos de instancias disponibles que son compatibles con los EFA en una región, utilice el comando describe-instance-types con el

parámetro `--region`. Incluya el parámetro `--filters` para limitar los resultados a los tipos de instancia que admiten EFA y el parámetro `--query` para limitar la salida al valor de `InstanceType`.

```
aws ec2 describe-instance-types  --region us-east-1  --filters Name=network-info.efa-
supported,Values=true  --query "InstanceTypes[*].[InstanceType]"  --output text | sort
```

Sistemas operativos compatibles

Los siguientes sistemas operativos admiten EFA con tipos de instancias basados en Intel/AMD x86:

- Amazon Linux 2023
- Amazon Linux 2
- CentOS 7
- RHEL 7, 8 y 9
- Debian 10 y 11
- Rocky Linux 8 y 9
- Ubuntu 20.04 y 22.04
- SUSE Linux Enterprise 15 SP2 y posteriores
- OpenSUSE Leap 15.4 y versiones posteriores

> **Note**
>
> Ubuntu 20.04 admite el soporte directo entre pares cuando se usa con instancias `dl1.24xlarge`.

Los siguientes sistemas operativos admiten EFA con tipos de instancias basados en Arm (Graviton):

- Amazon Linux 2023
- Amazon Linux 2
- RHEL 8 y 9 y Rocky Linux 8 y 9
- Debian 10 y 11
- Ubuntu 20.04 y 22.04
- SUSE Linux Enterprise 15 SP2 y posteriores

Limitaciones de EFA

Los EFA presentan las siguientes limitaciones:

- Todos los tipos de instancias P4d y P5 admiten NVIDIA GPUDirect Remote Direct Memory Access (RDMA).
- Actualmente, no se admite el tráfico EFA entre las instancias P4d/P4de/DL1 y otros tipos de instancias.
- Los tipos de instancias que admiten varias tarjetas de red se pueden configurar con un EFA por tarjeta de red. Todos los demás tipos de instancia compatibles admiten solo un EFA por instancia.
- Los hosts dedicados y las instancias dedicadas de `c7g.16xlarge`, `m7g.16xlarge` y `r7g.16xlarge` no son compatibles cuando se adjunta un EFA.
- El tráfico de omisión del sistema operativo de EFA se limita a una única subred. En otras palabras, el tráfico de EFA no se puede enviar de una subred a otra. El tráfico de IP normal desde el EFA se puede enviar de una subred a otra.
- El tráfico de omisión de sistema operativo de EFA no es enrutable. El tráfico de IP normal desde el EFA sigue siendo enrutable.
- El EFA debe formar parte de un grupo de seguridad que permita todo el tráfico entrante y saliente hacia y desde el propio grupo de seguridad.
- No se admite EFA en las instancias de Windows.
- EFA no es compatible con AWS Outposts.

Precios de EFA

EFA está disponible como una función de red opcional de Amazon EC2 que puede habilitar en cualquier instancia compatible sin costo adicional.

Introducción a las instancias P5 y EFA

Las instancias P5 ofrecen 3200 Gbps de ancho de banda de la red mediante el uso de varias interfaces EFA. Las instancias P5 admiten 32 tarjetas de red. Si necesita más información sobre cómo empezar a trabajar con las instancias P5, consulte Introducción a las instancias P5 para Linux.

Le recomendamos que defina una única interfaz de red EFA por tarjeta de red. Para configurar estas interfaces en el momento de la inicialización, recomendamos los siguientes ajustes:

- Para la interfaz de red `0`, especifique el índice de dispositivos `0`.

- Para las interfaces de red de 1 a 31, especifique el índice de dispositivos 1.

Si utiliza la consola de Amazon EC2, en el Asistente de inicialización de instancias, elija Editar en la sección Configuración de red. Expanda Configuración de red avanzada y elija Agregar interfaz de red para agregar el número necesario de interfaces de red. Para cada interfaz de red, en EFA, seleccione Habilitar. Para todas las interfaces de red, excepto la interfaz de red principal, en Índice de dispositivos, especifique 1. Configure los demás ajustes según sea necesario.

Si está utilizando la AWS CLI, utilice el comando run-instances; en `--network-interfaces`, especifique el número requerido de interfaces de red. Para cada interfaz de red, en `InterfaceType`, especifique `efa`. Para la interfaz de red principal, en `NetworkCardIndex` y `DeviceIndex`, especifique `0`. Para las demás interfaces de red, en `NetworkCardIndex`, especifique un valor único de 1 a 31 y, en `DeviceIndex`, especifique 1.

En el siguiente fragmento de comando de ejemplo, se muestra una solicitud con 32 interfaces de red EFA.

```
$ aws --region $REGION ec2 run-instances \
 --instance-type p5.48xlarge \
 --count 1 \
 --key-name key_pair_name \
 --image-id ami_id \
 --network-interfaces
 "NetworkCardIndex=0,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \

 "NetworkCardIndex=1,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \

 "NetworkCardIndex=2,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \

 "NetworkCardIndex=3,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \

 "NetworkCardIndex=4,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \

 "NetworkCardIndex=5,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \
```

```
"NetworkCardIndex=6,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
\
"NetworkCardIndex=7,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
\
"NetworkCardIndex=8,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
\
"NetworkCardIndex=9,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
\
"NetworkCardIndex=10,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\
"NetworkCardIndex=11,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\
"NetworkCardIndex=12,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\
"NetworkCardIndex=13,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\
"NetworkCardIndex=14,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\
"NetworkCardIndex=15,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\
"NetworkCardIndex=16,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\
"NetworkCardIndex=17,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\
"NetworkCardIndex=18,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\
"NetworkCardIndex=19,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\
```

```
  "NetworkCardIndex=20,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
  \
  "NetworkCardIndex=21,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
  \
  "NetworkCardIndex=22,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
  \
  "NetworkCardIndex=23,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
  \
  "NetworkCardIndex=24,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
  \
  "NetworkCardIndex=25,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
  \
  "NetworkCardIndex=26,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
  \
  "NetworkCardIndex=27,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
  \
  "NetworkCardIndex=28,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
  \
  "NetworkCardIndex=29,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
  \
  "NetworkCardIndex=30,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
  \
  "NetworkCardIndex=31,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
...
```

Si utiliza una plantilla de inicialización, especifique el número necesario de interfaces de red en la plantilla de inicialización. Para cada interfaz de red, en `InterfaceType`, especifique `efa`. Para la interfaz de red principal, en `NetworkCardIndex` y `DeviceIndex`, especifique `0`. Para las demás interfaces de red, en `NetworkCardIndex`, especifique un valor único de 1 a 31 y,

en `DeviceIndex`, especifique 1. En el siguiente fragmento, se muestra un ejemplo con 3 interfaces de red de las 32 interfaces de red posibles.

```
"NetworkInterfaces":[
{
  "NetworkCardIndex":0,
  "DeviceIndex":0,
  "InterfaceType": "efa",
  "AssociatePublicIpAddress":false,
  "Groups":[
    "security_group_id"
  ],
  "DeleteOnTermination":true
},
{
  "NetworkCardIndex": 1,
  "DeviceIndex": 1,
  "InterfaceType": "efa",
  "AssociatePublicIpAddress":false,
  "Groups":[
    "security_group_id"
  ],
  "DeleteOnTermination":true
},
{
  "NetworkCardIndex": 2,
  "DeviceIndex": 1,
  "InterfaceType": "efa",
  "AssociatePublicIpAddress":false,
  "Groups":[
    "security_group_id"
  ],
  "DeleteOnTermination":true
}
...
```

Al iniciar una instancia P5 con más de una interfaz de red, no puede asignar automáticamente direcciones IP públicas. Sin embargo, puede adjuntar una dirección IP elástica a la interfaz de red principal (NetworkCardIndex=0, DeviceIndex=0) después de la inicialización para la conectividad a Internet. Tanto Ubuntu 20.04 y versiones posteriores como Amazon Linux 2 y versiones posteriores están configurados para usar la interfaz de red principal para el tráfico de Internet cuando se inicia la instancia, tal como se recomendó anteriormente.

Introducción a EFA y MPI

Este tutorial le ayuda a iniciar un clúster de instancias habilitado para MPI y EFA para cargas de trabajo de HPC. En este tutorial, seguirá estos pasos:

Contenido

Paso 1: preparar un grupo de seguridad habilitado para EFA

Un EFA requiere un grupo de seguridad que permita todo el tráfico entrante y saliente hacia y desde el propio grupo de seguridad. En el siguiente procedimiento, se crea un grupo de seguridad que permite todo el tráfico entrante y saliente de sí mismo, y que permite el tráfico SSH entrante desde cualquier dirección IPv4 para la conectividad SSH.

> **Important**
>
> Este grupo de seguridad está pensado solo con fines de prueba. Para sus entornos de producción, le recomendamos que cree una regla SSH entrante que permita el tráfico únicamente desde la dirección IP desde la que se conecta, como la dirección IP de su equipo o un rango de direcciones IP en la red local.

Para ver otros escenarios, consulte Reglas de grupo de seguridad para diferentes casos de uso.

Para crear un grupo de seguridad habilitado para EFA

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Grupos de seguridad y, a continuación, elija Crear grupo de seguridad.
3. En la ventana Crear grupo de seguridad, haga lo siguiente:
   a. En Nombre del grupo de seguridad, ingrese un nombre descriptivo para el grupo de seguridad, como, por ejemplo, `EFA-enabled security group`.
   b. (Opcional) En Descripción, ingrese una breve descripción del grupo de seguridad.
   c. En VPC, seleccione la VPC en la que desea iniciar sus instancias habilitadas para EFA.
   d. Elija Crear grupo de seguridad.
4. Seleccione el grupo de seguridad que creó y, en la pestaña Detalles, copie el ID del grupo de seguridad.
5. Con el grupo de seguridad todavía seleccionado, elija Acciones, Editar reglas de entrada y, luego, haga lo siguiente:
   a. Seleccione Agregar regla.
   b. En Tipo, seleccione Todo el tráfico.
   c. En Tipo de origen, elija Personalizar y pegue el ID del grupo de seguridad que copió en el campo.
   d. Seleccione Agregar regla.
   e. En Tipo, seleccione SSH.
   f. En Tipo de origen, elija Cualquiera de IPv4.
   g. Seleccione Guardar reglas.
6. Con el grupo de seguridad todavía seleccionado, elija Acciones, Editar reglas de salida y, luego, haga lo siguiente:
   a. Seleccione Agregar regla.
   b. En Tipo, seleccione Todo el tráfico.
   c. En Tipo de destino, elija Personalizar y pegue el ID del grupo de seguridad que copió en el campo.
   d. Seleccione Guardar reglas.

Paso 2: iniciar una instancia temporal

Lance una instancia temporal que puede utilizar para instalar y configurar los componentes de software de EFA. Puede utilizar esta instancia para crear una AMI habilitada para EFA desde la que puede iniciar sus instancias habilitadas para EFA.

Para iniciar una instancia temporal

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instancias y, a continuación, Iniciar instancias para abrir el nuevo asistente de inicialización de instancias.
3. (Opcional) En la sección Nombre y etiquetas, proporcione un nombre para la instancia, como `EFA-instance`. El nombre se asigna a la instancia como etiqueta de recurso (`Name=`*`EFA-instance`*).
4. En la sección Application and OS Images (Imágenes de aplicaciones y sistema operativo), seleccione una AMI para uno de los sistemas operativos compatibles.
5. En la sección Tipo de instancia, seleccione el tipo de instancia admitida.
6. En la sección Par de claves, seleccione el par de claves que desea utilizar en la instancia.
7. En la sección Configuración de red, elija Editar y realice lo siguiente:
   a. En Subred, elija la subred en la que desea iniciar la instancia. Si no selecciona una subred, no puede habilitar la instancia para EFA.
   b. En Firewall (grupos de seguridad), elija Seleccionar grupo de seguridad existente y, a continuación, seleccione el grupo de seguridad que creó en el paso anterior.
   c. Expanda la sección Configuración avanzada de la red y en Elastic Fabric Adapter, seleccione Habilitar.
8. En la sección Almacenamiento, configure los volúmenes según sea necesario.
9. En el panel Resumen que se encuentra a la derecha, elija Iniciar instancia.

Paso 3: instalar el software EFA

Instale el kernel habilitado para EFA, los controladores de EFA, Libfabric y la pila Open MPI necesarios para admitir EFA en su instancia temporal.

Los pasos varían en función de si pretende utilizar EFA con Open MPI, con Intel MPI o con Open MPI e Intel MPI.

Para instalar el software EFA

1. Conéctese a la instancia que lanzó. Para obtener más información, consulte Conexión con la instancia de Linux.
2. Para asegurarse de que todos los paquetes de software están actualizados, realice una actualización rápida del software en la instancia. Este proceso puede demorar unos minutos.

   - Amazon Linux 2023, Amazon Linux 2, RHEL 7/8/9, CentOS 7, Rocky Linux 8/9

     ```
     $ sudo yum update -y
     ```

   - Ubuntu 20.04/22.04 y Debian 10/11

     ```
     $ sudo apt-get update && sudo apt-get upgrade -y
     ```

   - SUSE Linux Enterprise

     ```
     $ sudo zypper update -y
     ```

3. Reinicie la instancia y vuelva a conectarse a ella.
4. Descargue los archivos de instalación de software de EFA. Los archivos de instalación de software están empaquetados en un archivo tarball comprimido (`.tar.gz`). Para descargar la última versión estable, utilice el comando siguiente.

   ```
   $ C:\> curl -O https://efa-installer.amazonaws.com/aws-efa-installer-1.32.0.tar.gz
   ```

   También puede obtener la última versión reemplazando el número de versión por `latest` en el comando anterior.
5. (Opcional) Verifique la autenticidad y la integridad del archivo tarball (`.tar.gz`) de EFA.

   Le recomendamos que lo haga para verificar la identidad del editor de software y para verificar que el archivo no se haya modificado ni dañado desde que se publicó. Si no desea verificar el archivo tarball, omita este paso.

> **Note**
>
> De forma alternativa, si prefiere verificar el archivo tarball con una suma de comprobación MD5 o SHA256, consulte Verificar el instalador de EFA mediante una suma de comprobación.

a. Descargue la clave pública de GPG e impórtela a su conjunto de claves.

```
$ wget https://efa-installer.amazonaws.com/aws-efa-installer.key && gpg --
import aws-efa-installer.key
```

El comando debe devolver un valor de clave. Anote el valor de clave, ya que lo necesitará en el siguiente paso.

b. Verifique la huella digital de la clave de GPG. Ejecute el siguiente comando y especifique el valor de clave del paso anterior.

```
$ gpg --fingerprint key_value
```

El comando debe devolver una huella digital idéntica a `4E90 91BC BB97 A96B 26B1 5E59 A054 80B1 DD2D 3CCC`. Si la huella digital no coincide, no ejecute el script de instalación de EFA y contáctese con AWS Support.

c. Descargue el archivo de firma y verifique la firma del archivo tarball de EFA.

```
$ wget https://efa-installer.amazonaws.com/aws-efa-installer-1.32.0.tar.gz.sig
 && gpg --verify ./aws-efa-installer-1.32.0.tar.gz.sig
```

A continuación se muestra un ejemplo de salida.

```
gpg: Signature made Wed 29 Jul 2020 12:50:13 AM UTC using RSA key ID DD2D3CCC
gpg: Good signature from "Amazon EC2 EFA <ec2-efa-maintainers@amazon.com>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 4E90 91BC BB97 A96B 26B1  5E59 A054 80B1 DD2D 3CCC
```

Si el resultado incluye `Good signature` y la huella digital coincide con la huella digital del paso anterior, avance al siguiente paso. Si no es así, no ejecute el script de instalación de EFA y contáctese con AWS Support.

6. Extraiga los archivos desde el archivo `.tar.gz` comprimido y acceda al directorio extraído.

```
$ C:\> tar -xf aws-efa-installer-1.32.0.tar.gz && cd aws-efa-installer
```

7. Instale el software EFA. Realice una de las siguientes acciones en función de su caso de uso.

> **Note**
>
> EFA no admite NVIDIA GPUDirect con SUSE Linux. Si usa SUSE Linux, debe especificar adicionalmente la opción `--skip-kmod` para evitar la instalación de kmod. De forma predeterminada, SUSE Linux no permite módulos de kernel fuera del árbol.

Open MPI and Intel MPI

Si tiene la intención de usar EFA con Open MPI e Intel MPI, debe instalar el software de EFA con Libfabric y Open MPI, y debe completar el paso 5: Instalar Intel MPI.

Para instalar el software EFA con Libfabric y Open MPI, ejecute el siguiente comando.

> **Note**
>
> A partir de la versión 1.30.0 de EFA, tanto Open MPI 4 como Open MPI 5 se instalan de forma predeterminada. Si lo desea, puede especificar la versión de Open MPI que desea instalar. Para instalar únicamente Open MPI 4, incluya `--mpi=openmpi4`. Para instalar únicamente Open MPI 5, incluya `--mpi=openmpi5`. Para instalar ambos, omita la opción `--mpi`.

```
$ C:\> sudo ./efa_installer.sh -y
```

Libfabric se instala en `/opt/amazon/efa`. Open MPI 4 se instala en `/opt/amazon/openmpi`. Open MPI 5 se instala en `/opt/amazon/openmpi5`.

Open MPI only

Si tiene la intención de usar EFA solo con Open MPI, debe instalar el software de EFA con Libfabric y Open MPI, y debe omitir el paso 5: Instalar Intel MPI. Para instalar el software EFA con Libfabric y Open MPI, ejecute el siguiente comando.

> **Note**
>
> A partir de la versión 1.30.0 de EFA, tanto Open MPI 4 como Open MPI 5 se instalan de forma predeterminada. Si lo desea, puede especificar la versión de Open MPI que desea instalar. Para instalar únicamente Open MPI 4, incluya `--mpi=openmpi4`. Para instalar únicamente Open MPI 5, incluya `--mpi=openmpi5`. Para instalar ambos, omita la opción `--mpi`.

```
$ C:\> sudo ./efa_installer.sh -y
```

Libfabric se instala en `/opt/amazon/efa`. Open MPI 4 se instala en `/opt/amazon/openmpi`. Open MPI 5 se instala en `/opt/amazon/openmpi5`.

Intel MPI only

Si tiene la intención de utilizar solo EFA con Intel MPI, puede instalar el software EFA sin Libfabric y Open MPI. En este caso, Intel MPI utiliza su Libfabric integrado. Si decide hacerlo, debe completar el paso 5: Instalar Intel MPI.

Para instalar el software EFA sin Libfabric y Open MPI, ejecute el siguiente comando.

```
$ C:\> sudo ./efa_installer.sh -y --minimal
```

8. Si el instalador de EFA le pide que reinicie la instancia, hágalo y vuelva a conectarse a la instancia. De lo contrario, cierre la sesión de la instancia y vuelva a iniciar sesión para completar la instalación.

Paso 4: (opcional) habilitar Open MPI 5

> **Note**
>
> Realice este paso solo si pretende usar Open MPI 5.

A partir de la versión 1.30.0 de EFA, tanto Open MPI 4 como Open MPI 5 se instalan de forma predeterminada. Como alternativa, puede elegir instalar solo Open MPI 4 o Open MPI 5.

Si optó por instalar Open MPI 5 en el paso 3: Instalar el software de EFA y tiene intención de usarlo, debe realizar los siguientes pasos para habilitarlo.

Habilitar Open MPI 5

1. Agregue Open MPI 5 a la variable de entorno PATH.

   ```
   $ module load openmpi5
   ```

2. Compruebe que Open MPI 5 esté habilitado para su uso.

   ```
   $ which mpicc
   ```

   El comando debería devolver el directorio de instalación de Open MPI 5: `/opt/amazon/openmpi5`.

3. (Opcional) Para asegurarse de que Open MPI 5 se agregue a la variable de entorno PATH cada vez que se inicie la instancia, haga lo siguiente:

   bash shell

   Agregue `module load openmpi5` a `/home/`*`username`*`/.bashrc` y `/home/`*`username`*`/.bash_profile`.

   csh and tcsh shells

   Agregue `module load openmpi5` a `/home/`*`username`*`/.cshrc`.

Si necesita eliminar Open MPI 5 de la variable de entorno PATH, ejecute el siguiente comando y elimine el comando de los scripts de inicio del intérprete de comandos.

```
$ module unload openmpi5
```

Paso 5: (opcional) instalar Intel MPI

> **Important**
>
> Ejecute este paso solo si pretende utilizar Intel MPI. Si tiene la intención de utilizar solo Open MPI, omita este paso.

La instalación de Intel MPI requiere una instalación adicional y la configuración de una variable de entorno.

Requisito previo

Asegúrese de que el usuario que lleva a cabo los pasos siguientes tenga permisos sudo.

Para instalar Intel MPI

1. Para descargar el script de instalación de Intel MPI, haga lo siguiente:
   a. Visite el sitio web de Intel.
   b. En la sección Biblioteca de Intel MPI de la página web, elija el enlace para el instalador de la Biblioteca de Intel MPI para Linux sin conexión.
2. Ejecute el script de instalación que descargó en el paso anterior.

   ```
   $ C:\> sudo bash installation_script_name.sh
   ```
3. En el instalador, elija Aceptar e instalar.
4. Lea el programa de mejora de Intel, elija la opción correspondiente y, a continuación, Comenzar la instalación.
5. Cuando finalice la instalación, elija Cerrar.
6. De forma predeterminada, Intel MPI utiliza su Libfabric integrada (interna). En cambio, puede configurar Intel MPI para que use la Libfabric que se incluye con el instalador de EFA. Por lo general, el instalador de EFA incluye una versión de Libfabric posterior a la de Intel MPI. En algunos casos, la Libfabric que se incluye con el instalador de EFA es más eficaz que la de Intel MPI. Para configurar Intel MPI de modo que use la Libfabric que se incluye con el instalador de EFA, realice alguna de las siguientes acciones en función de su shell.

bash shells

Agregue la siguiente instrucción a /home/*username*/.bashrc y /home/*username*/.bash_profile.

```
export I_MPI_OFI_LIBRARY_INTERNAL=0
```

csh and tcsh shells

Agregue la siguiente instrucción a /home/*username*/.cshrc.

```
setenv I_MPI_OFI_LIBRARY_INTERNAL 0
```

7. Agregue el siguiente comando de origen al script de shell para obtener el script `vars.sh` desde el directorio de instalación para configurar el entorno del compilador cada vez que se inicie la instancia. Haga lo siguiente en función del shell.

   bash shells

   Agregue la siguiente instrucción a /home/*username*/.bashrc y /home/*username*/.bash_profile.

   ```
   source /opt/intel/oneapi/mpi/latest/env/vars.sh
   ```

   csh and tcsh shells

   Agregue la siguiente instrucción a /home/*username*/.cshrc.

   ```
   source /opt/intel/oneapi/mpi/latest/env/vars.csh
   ```

8. De forma predeterminada, si el EFA no está disponible debido a una configuración incorrecta, Intel MPI utilizará la pila de red TCP/IP, lo que puede provocar un rendimiento más lento de la aplicación. Puede evitar que esto suceda configurando `I_MPI_OFI_PROVIDER` en `efa`. Esto hace que Intel MPI falle con el siguiente error si el EFA no está disponible:

   ```
   Abort (XXXXXX) on node 0 (rank 0 in comm 0): Fatal error in PMPI_Init: OtherMPI
    error,
   MPIR_Init_thread (XXX).......:
   MPID_Init (XXXX).............:
   ```

```
MPIDI_OFI_mpi_init_hook (XXXX):
open_fabric (XXXX).............:
find_provider (XXXX)..........:
OFI fi_getinfo() failed (ofi_init.c:2684:find_provider:
```

Haga lo siguiente en función del shell.

bash shells

Agregue la siguiente instrucción a /home/*username*/.bashrc y /home/*username*/.bash_profile.

```
export I_MPI_OFI_PROVIDER=efa
```

csh and tcsh shells

Agregue la siguiente instrucción a /home/*username*/.cshrc.

```
setenv I_MPI_OFI_PROVIDER efa
```

9. De forma predeterminada, Intel MPI no imprime la información de depuración. Puede especificar diferentes niveles de detalle para controlar la información de depuración. Los valores posibles (ordenados en función de la cantidad de información que proporcionan) son los siguientes: `0` (predeterminado), `1`, `2`, `3`, `4`, `5`. El nivel `1` y los niveles superiores imprimen la `libfabric version` y el `libfabric provider`. Use la `libfabric version` para comprobar si Intel MPI utiliza la Libfabric interna o la Libfabric que se incluye con el instalador de EFA. Si utiliza la Libfabric interna, la versión llevará el sufijo `impi`. Use el `libfabric provider` para comprobar si Intel MPI utiliza el EFA o la red TCP/IP. Si utiliza el EFA, el valor será `efa`. Si utiliza la red TCP/IP, el valor será `tcp;ofi_rxm`.

   Para habilitar la información de depuración, realice alguna de las siguientes acciones en función del shell.

   bash shells

   Agregue la siguiente instrucción a /home/*username*/.bashrc y /home/*username*/.bash_profile.

   ```
   export I_MPI_DEBUG=value
   ```

csh and tcsh shells

Agregue la siguiente instrucción a /home/*username*/.cshrc.

```
setenv I_MPI_DEBUG value
```

10. De forma predeterminada, Intel MPI utiliza la memoria compartida del sistema operativo (shm) para la comunicación dentro del nodo y, por otro lado, usa la Libfabric (ofi) solo para la comunicación entre nodos. Por lo general, esta configuración proporciona el mejor rendimiento. Sin embargo, en algunos casos, la estructura shm de Intel MPI puede provocar el bloqueo de ciertas aplicaciones de forma indefinida.

    Para resolver este problema, puede forzar que Intel MPI use Libfabric para la comunicación tanto dentro del nodo como entre nodos. Para ello, realice alguna de las siguientes acciones en función del shell.

    bash shells

    Agregue la siguiente instrucción a /home/*username*/.bashrc y /home/*username*/.bash_profile.

    ```
    export I_MPI_FABRICS=ofi
    ```

    csh and tcsh shells

    Agregue la siguiente instrucción a /home/*username*/.cshrc.

    ```
    setenv I_MPI_FABRICS ofi
    ```

    > **Note**
    >
    > El proveedor de la Libfabric del EFA utiliza la memoria compartida del sistema operativo para la comunicación dentro del nodo. Esto significa que la configuración de I_MPI_FABRICS en ofi produce un rendimiento similar a la configuración predeterminada de shm:ofi.

11. Cierre la sesión de la instancia y, a continuación, vuelva a iniciar sesión.

Si ya no desea utilizar Intel MPI, quite las variables de entorno de los scripts de inicio del shell.

Paso 6: deshabilitar la protección ptrace

Para mejorar el rendimiento de la aplicación HPC, Libfabric utiliza la memoria local de la instancia para las comunicaciones entre procesos cuando los procesos se ejecutan en la misma instancia.

La característica de memoria compartida utiliza Cross Memory Attach (CMA), que no es compatible con la protección ptrace. Si utiliza una distribución Linux que tiene la protección ptrace habilitada de forma predeterminada, como Ubuntu, debe deshabilitarla. Si su distribución Linux no tiene la protección ptrace habilitada de forma predeterminada, omita este paso.

Para deshabilitar la protección ptrace

Aplique alguna de las siguientes acciones:

- Para deshabilitar temporalmente la protección ptrace con fines de prueba, ejecute el siguiente comando.

```
$ sudo sysctl -w kernel.yama.ptrace_scope=0
```

- Para deshabilitar permanentemente la protección ptrace, agregue `kernel.yama.ptrace_scope = 0` `/etc/sysctl.d/10-ptrace.conf` y reinicie la instancia.

Paso 7. Confirmar instalación

Para confirmar que la instalación se ha realizado correctamente

1. Para confirmar que MPI se instaló correctamente, ejecute el comando siguiente:

```
$ which mpicc
```

   - En el caso de Open MPI, la ruta devuelta debe incluir `/opt/amazon/`
   - En el caso de Intel MPI, la ruta devuelta debe incluir `/opt/intel/`. Si no obtiene el resultado esperado, asegúrese de haber obtenido el script `vars.sh` de Intel MPI.

2. Para confirmar que los componentes de software de EFA y Libfabric se instalaron correctamente, ejecute el siguiente comando.

```
$ C:\> fi_info -p efa -t FI_EP_RDM
```

El comando debe devolver información acerca de las interfaces de EFA de Libfabric. En el siguiente ejemplo, se muestra el comando de salida.

```
provider: efa
    fabric: EFA-fe80::94:3dff:fe89:1b70
    domain: efa_0-rdm
    version: 2.0
    type: FI_EP_RDM
    protocol: FI_PROTO_EFA
```

Paso 8: instalar la aplicación de HPC

Instale la aplicación de HPC en la instancia temporal. El procedimiento de instalación varía en función de la aplicación de HPC específica. Para obtener más información, consulte Manage software on your AL2 instance en la Guía del usuario de Amazon Linux 2.

> **Note**
>
> Consulte la documentación de su aplicación de HPC para ver las instrucciones de instalación.

Paso 9: crear una AMI habilitada para EFA

Después de haber instalado los componentes de software requeridos, crea una AMI que puede reutilizar para iniciar las instancias habilitadas para EFA.

Para crear una AMI desde la instancia temporal

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancias).
3. Seleccione la instancia temporal que creó y elija Acciones, Imagen, Crear imagen.
4. En Crear imagen, realice lo siguiente:
   a. En Nombre de imagen, ingrese un nombre descriptivo para la AMI.
   b. (Opcional) En Descripción de imagen, ingrese una breve descripción del propósito la AMI.
   c. Elija Crear imagen.

5. En el panel de navegación, elija AMI.
6. Localice la AMI que creó en la lista. Espere a que el estado pase de `pending` a `available` antes de continuar con el paso siguiente.

Paso 10: iniciar instancias habilitadas para EFA en un grupo con ubicación en clúster

Lance las instancias habilitadas para EFA en un grupo de ubicación en clúster utilizando la AMI habilitada para EFA que creó en el Paso 7 y el grupo de seguridad habilitado para EFA que creó en el Paso 1.

> **Note**
>
> - No es un requisito absoluto iniciar las instancias habilitadas con un EFA a un grupo con ubicación en clúster. Sin embargo, le recomendamos ejecutar sus instancias habilitadas para EFA en un grupo con ubicación en clúster a medida que inicia las instancias en un grupo de baja latencia en una única zona de disponibilidad.
> - Para garantizar que la capacidad esté disponible a medida que escala las instancias del clúster, puede crear una reserva de capacidad para su grupo con ubicación en clúster. Para obtener más información, consulte Las reservas de capacidad en grupos con ubicación en clúster.

Para iniciar una instancia temporal

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instancias y, a continuación, Iniciar instancias para abrir el nuevo asistente de inicialización de instancias.
3. (Opcional) En la sección Nombre y etiquetas, proporcione un nombre para la instancia, como `EFA-instance`. El nombre se asigna a la instancia como etiqueta de recurso (`Name=`*`EFA-instance`*).
4. En la sección Imágenes de aplicaciones y sistema operativo, elija Mis AMI y, a continuación, seleccione la AMI que creó en el paso anterior.
5. En la sección Tipo de instancia, seleccione el tipo de instancia admitida.
6. En la sección Par de claves, seleccione el par de claves que desea utilizar en la instancia.
7. En la sección Configuración de red, elija Editar y realice lo siguiente:

a. En Subred, elija la subred en la que desea iniciar la instancia. Si no selecciona una subred, no puede habilitar la instancia para EFA.

b. En Firewall (grupos de seguridad), elija Seleccionar grupo de seguridad existente y, a continuación, seleccione el grupo de seguridad que creó en el paso anterior.

c. Expanda la sección Advanced network configuration (Configuración avanzada de la red) y en Elastic Fabric Adapter, seleccione Enable (Habilitar).

8. (Opcional) En la sección Almacenamiento, configure los volúmenes según sea necesario.
9. En la sección Detalles avanzados, para Nombre del grupo de ubicación, seleccione el grupo con ubicación en clúster en el que se iniciarán las instancias. Si necesita crear un nuevo grupo con ubicación en clúster, elija Crear nuevo grupo de ubicación.
10. En el panel Resumenque se encuentra a la derecha, en Cantidad de instancias, ingrese la cantidad de instancias habilitadas para EFA que desea iniciar y, a continuación, elija Iniciar instancias.

Paso 11: terminar la instancia temporal

En este punto, ya no necesita la instancia temporal que lanzó. Puede terminar la instancia para dejar de incurrir en cargos debido a esta.

Para terminar la instancia temporal

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancias).
3. Seleccione la instancia temporal que creó y, a continuación, elija Acciones, Estado de instancia, Terminar instancia.
4. Cuando se le indique que confirme, elija Rescindir.

Paso 12: habilitar SSH sin contraseña

Para permitir que las aplicaciones se ejecuten en todas las instancias del clúster, debe habilitar el acceso mediante SSH sin contraseña desde el nodo principal hasta los nodos miembro. El nodo principal es la instancia desde la que se ejecutan las aplicaciones. Las instancias restantes del clúster son los nodos miembros.

Para habilitar SSH sin contraseña entre las instancias del clúster

1. Seleccione una instancia del clúster como nodo principal y conéctese a ella.
2. Desactive `strictHostKeyChecking` y habilite `ForwardAgent` en el nodo principal. Abra `~/.ssh/config` con su editor de texto preferido y agregue lo siguiente.

   ```
   Host *
       ForwardAgent yes
   Host *
       StrictHostKeyChecking no
   ```

3. Genere un par de claves de RSA.

   ```
   $ ssh-keygen -t rsa -N "" -f ~/.ssh/id_rsa
   ```

   El par de claves se crea en el directorio `$HOME/.ssh/`.
4. Cambie los permisos de la clave privada en el nodo principal.

   ```
   $ chmod 600 ~/.ssh/id_rsa
   chmod 600 ~/.ssh/config
   ```

5. Abra `~/.ssh/id_rsa.pub` con su editor de texto preferido y copie la clave.
6. Para cada nodo miembro del clúster, realice lo siguiente:

   a. Conéctese a la instancia.

   b. Abra `~/.ssh/authorized_keys` con su editor de texto preferido y agregue la clave pública que copió anteriormente.
7. Para probar que SSH sin contraseña funciona como se esperaba, conecte al nodo principal y ejecute el siguiente comando.

   ```
   $ ssh member_node_private_ip
   ```

   Debe conectarse al nodo miembro sin que se le pida una clave o una contraseña.

Introducción a EFA y NCCL

La Biblioteca de comunicación colectiva de NVIDIA (NCCL) es una biblioteca de rutinas de comunicación colectiva estándar para múltiples GPU en un solo nodo o múltiples nodos. NCCL se

puede usar junto con EFA, Libfabric y MPI para admitir varias cargas de trabajo de machine learning. Para obtener más información, consulte el sitio web de NCCL.

> **Note**
>
> - NCCL con EFA solo se admite con `p3dn.24xlarge`, `p4d.24xlarge` y `p5.48xlarge`.
> - Con EFA solo se admite NCCL 2.4.2 y versiones posteriores.

Los siguientes tutoriales le ayudan a iniciar un clúster de instancias habilitado para NCCL y EFA para cargas de trabajo de machine learning.

- Usar una base AMI
- Utilizar una AMI de aprendizaje profundo de AWS

Usar una base AMI

Los siguientes pasos le ayudarán a empezar a utilizar Elastic Fabric Adapter con una AMI para uno de los sistemas operativos base compatibles.

> **Note**
>
> - Solo se admiten los tipos de instancia `p3dn.24xlarge`, `p4d.24xlarge` y `p5.48xlarge`.
> - Solo se admiten las AMI base de Amazon Linux 2, RHEL 7/8/9, CentOS 7, Rocky Linux 8/9 y Ubuntu 20.04/22.04.

Contenido

Paso 1: preparar un grupo de seguridad habilitado para EFA

Un EFA requiere un grupo de seguridad que permita todo el tráfico entrante y saliente hacia y desde el propio grupo de seguridad. En el siguiente procedimiento, se crea un grupo de seguridad que permite todo el tráfico entrante y saliente de sí mismo, y que permite el tráfico SSH entrante desde cualquier dirección IPv4 para la conectividad SSH.

> **Important**
>
> Este grupo de seguridad está pensado solo con fines de prueba. Para sus entornos de producción, le recomendamos que cree una regla SSH entrante que permita el tráfico únicamente desde la dirección IP desde la que se conecta, como la dirección IP de su equipo o un rango de direcciones IP en la red local.

Para ver otros escenarios, consulte Reglas de grupo de seguridad para diferentes casos de uso.

Para crear un grupo de seguridad habilitado para EFA

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Grupos de seguridad y, a continuación, elija Crear grupo de seguridad.
3. En la ventana Crear grupo de seguridad, haga lo siguiente:
   a. En Nombre del grupo de seguridad, ingrese un nombre descriptivo para el grupo de seguridad, como, por ejemplo, `EFA-enabled security group`.
   b. (Opcional) En Descripción, ingrese una breve descripción del grupo de seguridad.

   c. En VPC, seleccione la VPC en la que desea iniciar sus instancias habilitadas para EFA.
   d. Elija Crear grupo de seguridad.
4. Seleccione el grupo de seguridad que creó y, en la pestaña Detalles, copie el ID del grupo de seguridad.
5. Con el grupo de seguridad todavía seleccionado, elija Acciones, Editar reglas de entrada y, luego, haga lo siguiente:
   a. Seleccione Agregar regla.
   b. En Tipo, seleccione Todo el tráfico.
   c. En Tipo de origen, elija Personalizar y pegue el ID del grupo de seguridad que copió en el campo.
   d. Seleccione Agregar regla.
   e. En Tipo, seleccione SSH.
   f. En Tipo de origen, elija Cualquiera de IPv4.
   g. Seleccione Guardar reglas.
6. Con el grupo de seguridad todavía seleccionado, elija Acciones, Editar reglas de salida y, luego, haga lo siguiente:
   a. Seleccione Agregar regla.
   b. En Tipo, seleccione Todo el tráfico.
   c. En Tipo de destino, elija Personalizar y pegue el ID del grupo de seguridad que copió en el campo.
   d. Seleccione Guardar reglas.

Paso 2: iniciar una instancia temporal

Lance una instancia temporal que puede utilizar para instalar y configurar los componentes de software de EFA. Puede utilizar esta instancia para crear una AMI habilitada para EFA desde la que puede iniciar sus instancias habilitadas para EFA.

Para iniciar una instancia temporal

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instancias y, a continuación, Iniciar instancias para abrir el nuevo asistente de inicialización de instancias.

3. (Opcional) En la sección Nombre y etiquetas, proporcione un nombre para la instancia, como `EFA-instance`. El nombre se asigna a la instancia como etiqueta de recurso (`Name=`*`EFA-instance`*).
4. En la sección Imágenes de aplicaciones y sistema operativo, seleccione una AMI para uno de los sistemas operativos compatibles.
5. En la sección Tipo de instancia, seleccione `p3dn.24xlarge`, `p4d.24xlarge` o `p5.48xlarge`.
6. En la sección Par de claves, seleccione el par de claves que desea utilizar en la instancia.
7. En la sección Configuración de red, elija Editar y realice lo siguiente:
   a. En Subred, elija la subred en la que desea iniciar la instancia. Si no selecciona una subred, no puede habilitar la instancia para EFA.
   b. En Firewall (grupos de seguridad), elija Seleccionar grupo de seguridad existente y, a continuación, seleccione el grupo de seguridad que creó en el paso anterior.
   c. Expanda la sección Configuración avanzada de la red y en Elastic Fabric Adapter, seleccione Habilitar.
8. En la sección Storage (Almacenamiento), configure los volúmenes según sea necesario.

   > **Note**
   >
   > Debe aprovisionar 10 a 20 GiB adicionales de almacenamiento para el conjunto de herramientas CUDA de Nvidia. Si no aprovisiona suficiente almacenamiento, recibirá un error de `insufficient disk space` cuando intente instalar los controladores de Nvidia y el kit de herramientas CUDA.

9. En el panel Resumen que se encuentra a la derecha, elija Iniciar instancia.

Paso 3: instalar los controladores de GPU Nvidia, el kit de herramientas Nvidia CUDA y la cuDNN

Amazon Linux 2

Para instalar los controladores de GPU Nvidia, el kit de herramientas Nvidia CUDA y la cuDNN, haga lo siguiente:

1. Para asegurarse de que todos los paquetes de software están actualizados, realice una actualización rápida del software en la instancia.

```
$ sudo yum upgrade -y && sudo reboot
```

Una vez que se haya reiniciado, vuelva a conectarse a la instancia.

2. Instale las utilidades necesarias para instalar los controladores de la GPU Nvidia y el kit de herramientas Nvidia CUDA.

```
$ sudo yum groupinstall 'Development Tools' -y
```

3. Desactive los controladores de código abierto de `nouveau`.

   a. Instale las utilidades y el paquete de encabezados del kernel necesarios para la versión del kernel que está ejecutando actualmente.

```
$ sudo yum install -y wget kernel-devel-$(uname -r) kernel-headers-$(uname -
r)
```

   b. Agregue `nouveau` al archivo de lista de denegaciones `/etc/modprobe.d/blacklist.conf` .

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

   c. Anexe `GRUB_CMDLINE_LINUX="rdblacklist=nouveau"` al archivo `grub` y vuelva a generar la configuración de Grub.

```
$ echo 'GRUB_CMDLINE_LINUX="rdblacklist=nouveau"' | sudo tee -a /etc/
default/grub \
&& sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

4. Reinicie la instancia y vuelva a conectarse a ella.
5. Preparar los repositorios necesarios

   a. Instale el repositorio EPEL para DKMS y habilite cualquier repositorio opcional para su distribución de Linux.

```
$ sudo yum install -y https://dl.fedoraproject.org/pub/epel/epel-release-
latest-7.noarch.rpm
```

b. Instale la clave GPG pública del repositorio CUDA.

```
$ distribution='rhel7'
```

c. Configure el repositorio de red CUDA y actualice la caché del repositorio.

```
$ ARCH=$( /bin/arch ) \
&& sudo yum-config-manager --add-repo http://developer.download.nvidia.com/
compute/cuda/repos/$distribution/${ARCH}/cuda-$distribution.repo \
&& sudo yum clean expire-cache
```

d. (Solo versión 5.10 del kernel) Siga estos pasos solo si está utilizando Amazon Linux 2 con la versión 5.10 del kernel. Si utiliza Amazon Linux 2 con la versión 4.12 del kernel, omita estos pasos. Para comprobar la versión del kernel, ejecute uname -r.

i. Cree el archivo de configuración del controlador de Nvidia denominado `/etc/dkms/nvidia.conf`.

```
$ sudo mkdir -p /etc/dkms \
&& echo "MAKE[0]=\"'make' -j2 module SYSSRC=\${kernel_source_dir}
 IGNORE_XEN_PRESENCE=1 IGNORE_PREEMPT_RT_PRESENCE=1 IGNORE_CC_MISMATCH=1
 CC=/usr/bin/gcc10-gcc\"" | sudo tee /etc/dkms/nvidia.conf
```

ii. (Solo para `p4d.24xlarge` y `p5.48xlarge`) Copie el archivo de configuración del controlador de Nvidia.

```
$ sudo cp /etc/dkms/nvidia.conf /etc/dkms/nvidia-open.conf
```

6. Instale los controladores de GPU de Nvidia, el conjunto de herramientas NVIDIA CUDA y la cuDNN.

- `p3dn.24xlarge`

```
$ sudo yum clean all \
&& sudo yum -y install kmod-nvidia-latest-dkms nvidia-driver-latest-dkms \
&& sudo yum -y install cuda-drivers-fabricmanager cuda libcudnn8-devel
```

- `p4d.24xlarge` y `p5.48xlarge`

```
$ sudo yum clean all \
&& sudo yum -y install kmod-nvidia-open-dkms nvidia-driver-latest-dkms \
&& sudo yum -y install cuda-drivers-fabricmanager cuda libcudnn8-devel
```

7. Reinicie la instancia y vuelva a conectarse a ella.
8. (Solo para `p4d.24xlarge` y `p5.48xlarge`) Inicie el servicio de Nvidia Fabric Manager y asegúrese de que se inicie de forma automática cuando se inicia la instancia. Nvidia Fabric Manager es necesario para la administración de NV Switch.

   ```
   $ sudo systemctl enable nvidia-fabricmanager && sudo systemctl start nvidia-
   fabricmanager
   ```

9. Asegúrese de que las rutas CUDA se establecen cada vez que se inicia la instancia.

   - Para intérpretes de comandos bash, agregue las siguientes instrucciones a `/home/`*`username`*`/.bashrc` y `/home/`*`username`*`/.bash_profile`.

     ```
     export PATH=/usr/local/cuda/bin:$PATH
     export LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
     lib64:$LD_LIBRARY_PATH
     ```

   - Para intérpretes de comandos tcsh, agregue las siguientes instrucciones a `/home/`*`username`*`/.cshrc`.

     ```
     setenv PATH=/usr/local/cuda/bin:$PATH
     setenv LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
     lib64:$LD_LIBRARY_PATH
     ```

10. Para confirmar que los controladores de la GPU Nvidia son funcionales, ejecute el siguiente comando.

    ```
    $ nvidia-smi -q | head
    ```

    El comando debe devolver información sobre las GPU de Nvidia, los controladores de GPU de Nvidia y el kit de herramientas Nvidia CUDA.

CentOS 7

Para instalar los controladores de GPU Nvidia, el kit de herramientas Nvidia CUDA y la cuDNN, haga lo siguiente:

1. Para asegurarse de que todos los paquetes de software están actualizados, realice una actualización rápida del software en la instancia.

   ```
   $ sudo yum upgrade -y && sudo reboot
   ```

   Una vez que se haya reiniciado, vuelva a conectarse a la instancia.

2. Instale las utilidades necesarias para instalar los controladores de la GPU Nvidia y el kit de herramientas Nvidia CUDA.

   ```
   $ sudo yum groupinstall 'Development Tools' -y \
   && sudo yum install -y tar bzip2 make automake pciutils elfutils-libelf-devel
    libglvnd-devel iptables firewalld vim bind-utils
   ```

3. Para usar el controlador de GPU Nvidia, primero debe deshabilitar los controladores de código abierto `nouveau`.

   a. Instale las utilidades y el paquete de encabezados del kernel necesarios para la versión del kernel que está ejecutando actualmente.

      ```
      $ sudo yum install -y wget kernel-devel-$(uname -r) kernel-headers-$(uname -
      r)
      ```

   b. Agregue `nouveau` al archivo de lista de denegaciones `/etc/modprobe.d/blacklist.conf` .

      ```
      $ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
      blacklist vga16fb
      blacklist nouveau
      blacklist rivafb
      blacklist nvidiafb
      blacklist rivatv
      EOF
      ```

   c. Abra `/etc/default/grub` con su editor de texto preferido y agregue lo siguiente.

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

d. Reconstruya la configuración de Grub.

```
$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

4. Reinicie la instancia y vuelva a conectarse a ella.
5. Instale los controladores de GPU de Nvidia, el conjunto de herramientas NVIDIA CUDA y la cuDNN.

   a. Instale el repositorio EPEL para DKMS y habilite cualquier repositorio opcional para su distribución de Linux.

   ```
   $ sudo yum install -y https://dl.fedoraproject.org/pub/epel/epel-release-
   latest-7.noarch.rpm
   ```

   b. Instale la clave GPG pública del repositorio CUDA.

   ```
   $ distribution='rhel7'
   ```

   c. Configure el repositorio de red CUDA y actualice la caché del repositorio.

   ```
   $ ARCH=$( /bin/arch ) \
   && sudo yum-config-manager --add-repo http://developer.download.nvidia.com/
   compute/cuda/repos/$distribution/${ARCH}/cuda-$distribution.repo \
   && sudo yum clean expire-cache
   ```

   d. Instale los controladores de NVIDIA, CUDA y la cuDNN.

   ```
   $ sudo yum clean all \
   && sudo yum -y install cuda-drivers-fabricmanager cuda libcudnn8-devel
   ```

6. Reinicie la instancia y vuelva a conectarse a ella.
7. (Solo para `p4d.24xlarge` y `p5.48xlarge`) Inicie el servicio de Nvidia Fabric Manager y asegúrese de que se inicie de forma automática cuando se inicia la instancia. Nvidia Fabric Manager es necesario para la administración de NV Switch.

   ```
   $ sudo systemctl start nvidia-fabricmanager \
   && sudo systemctl enable nvidia-fabricmanager
   ```

8. Asegúrese de que las rutas CUDA se establecen cada vez que se inicia la instancia.

   - Para intérpretes de comandos bash, agregue las siguientes instrucciones a /home/*username*/.bashrc y /home/*username*/.bash_profile.

     ```
     export PATH=/usr/local/cuda/bin:$PATH
     export LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
     lib64:$LD_LIBRARY_PATH
     ```

   - Para intérpretes de comandos tcsh, agregue las siguientes instrucciones a /home/*username*/.cshrc.

     ```
     setenv PATH=/usr/local/cuda/bin:$PATH
     setenv LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
     lib64:$LD_LIBRARY_PATH
     ```

9. Para confirmar que los controladores de la GPU Nvidia son funcionales, ejecute el siguiente comando.

   ```
   $ nvidia-smi -q | head
   ```

   El comando debe devolver información sobre las GPU de Nvidia, los controladores de GPU de Nvidia y el kit de herramientas Nvidia CUDA.

RHEL 7/8/9 and Rocky Linux 8/9

Para instalar los controladores de GPU Nvidia, el kit de herramientas Nvidia CUDA y la cuDNN, haga lo siguiente:

1. Para asegurarse de que todos los paquetes de software están actualizados, realice una actualización rápida del software en la instancia.

   ```
   $ sudo yum upgrade -y && sudo reboot
   ```

   Una vez que se haya reiniciado, vuelva a conectarse a la instancia.

2. Instale las utilidades necesarias para instalar los controladores de la GPU Nvidia y el kit de herramientas Nvidia CUDA.

```
$ sudo yum groupinstall 'Development Tools' -y
```

3. Para usar el controlador de GPU Nvidia, primero debe deshabilitar los controladores de código abierto nouveau.

   a. Instale las utilidades y el paquete de encabezados del kernel necesarios para la versión del kernel que está ejecutando actualmente.

   ```
   $ sudo yum install -y wget kernel-devel-$(uname -r) kernel-headers-$(uname -r)
   ```

   b. Agregue nouveau al archivo de lista de denegaciones `/etc/modprobe.d/blacklist.conf` .

   ```
   $ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
   blacklist vga16fb
   blacklist nouveau
   blacklist rivafb
   blacklist nvidiafb
   blacklist rivatv
   EOF
   ```

   c. Abra `/etc/default/grub` con su editor de texto preferido y agregue lo siguiente.

   ```
   GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
   ```

   d. Reconstruya la configuración de Grub.

   ```
   $ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
   ```

4. Reinicie la instancia y vuelva a conectarse a ella.
5. Instale los controladores de GPU de Nvidia, el conjunto de herramientas NVIDIA CUDA y la cuDNN.

   a. Instale el repositorio EPEL para DKMS y habilite cualquier repositorio opcional para su distribución de Linux.

   - RHEL 7

```
$ sudo yum install -y https://dl.fedoraproject.org/pub/epel/epel-release-
latest-7.noarch.rpm
```

- RHEL 8 y Rocky Linux 8/9

```
$ sudo yum install -y https://dl.fedoraproject.org/pub/epel/epel-release-
latest-8.noarch.rpm
```

- RHEL 9

```
$ sudo yum install -y https://dl.fedoraproject.org/pub/epel/epel-release-
latest-9.noarch.rpm
```

b. Instale la clave GPG pública del repositorio CUDA.

```
$ distribution=$(. /etc/os-release;echo $ID`rpm -E "%{?rhel}%{?fedora}"`)
```

c. Configure el repositorio de red CUDA y actualice la caché del repositorio.

```
$ ARCH=$( /bin/arch ) \
&& sudo yum-config-manager --add-repo http://developer.download.nvidia.com/
compute/cuda/repos/$distribution/${ARCH}/cuda-$distribution.repo \
&& sudo yum clean expire-cache
```

d. Instale los controladores de NVIDIA, CUDA y la cuDNN.

```
$ sudo yum clean all \
&& sudo yum -y install cuda-drivers-fabricmanager cuda libcudnn8-devel
```

6. Reinicie la instancia y vuelva a conectarse a ella.
7. (Solo para `p4d.24xlarge` y `p5.48xlarge`) Inicie el servicio de Nvidia Fabric Manager y asegúrese de que se inicie de forma automática cuando se inicia la instancia. Nvidia Fabric Manager es necesario para la administración de NV Switch.

```
$ sudo systemctl start nvidia-fabricmanager \
&& sudo systemctl enable nvidia-fabricmanager
```

8. Asegúrese de que las rutas CUDA se establecen cada vez que se inicia la instancia.

- Para intérpretes de comandos bash, agregue las siguientes instrucciones a /home/*username*/.bashrc y /home/*username*/.bash_profile.

```
export PATH=/usr/local/cuda/bin:$PATH
export LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
lib64:$LD_LIBRARY_PATH
```

- Para intérpretes de comandos tcsh, agregue las siguientes instrucciones a /home/*username*/.cshrc.

```
setenv PATH=/usr/local/cuda/bin:$PATH
setenv LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
lib64:$LD_LIBRARY_PATH
```

9. Para confirmar que los controladores de la GPU Nvidia son funcionales, ejecute el siguiente comando.

```
$ nvidia-smi -q | head
```

El comando debe devolver información sobre las GPU de Nvidia, los controladores de GPU de Nvidia y el kit de herramientas Nvidia CUDA.

Ubuntu 20.04/22.04

Para instalar los controladores de GPU Nvidia, el kit de herramientas Nvidia CUDA y la cuDNN, haga lo siguiente:

1. Para asegurarse de que todos los paquetes de software están actualizados, realice una actualización rápida del software en la instancia.

```
$ sudo apt-get update && sudo apt-get upgrade -y
```

2. Instale las utilidades necesarias para instalar los controladores de la GPU Nvidia y el kit de herramientas Nvidia CUDA.

```
$ sudo apt-get update && sudo apt-get install build-essential -y
```

3. Para usar el controlador de GPU Nvidia, primero debe deshabilitar los controladores de código abierto nouveau.

a. Instale las utilidades y el paquete de encabezados del kernel necesarios para la versión del kernel que está ejecutando actualmente.

```
$ sudo apt-get install -y gcc make linux-headers-$(uname -r)
```

b. Agregue nouveau al archivo de lista de denegaciones `/etc/modprobe.d/blacklist.conf` .

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

c. Abra `/etc/default/grub` con su editor de texto preferido y agregue lo siguiente.

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

d. Reconstruya la configuración de Grub.

```
$ sudo update-grub
```

4. Reinicie la instancia y vuelva a conectarse a ella.
5. Agregue el repositorio de CUD e instale los controladores de GPU de Nvidia, el conjunto de herramientas NVIDIA CUDA y la cuDNN.

   • `p3dn.24xlarge`

```
$ sudo apt-key adv --fetch-keys http://developer.download.nvidia.com/compute/
machine-learning/repos/ubuntu2004/x86_64/7fa2af80.pub \
&& wget -O /tmp/deeplearning.deb http://developer.download.nvidia.com/compute/
machine-learning/repos/ubuntu2004/x86_64/nvidia-machine-learning-repo-
ubuntu2004_1.0.0-1_amd64.deb \
&& sudo dpkg -i /tmp/deeplearning.deb \
&& wget -O /tmp/cuda.pin https://developer.download.nvidia.com/compute/cuda/
repos/ubuntu2004/x86_64/cuda-ubuntu2004.pin \
&& sudo mv /tmp/cuda.pin /etc/apt/preferences.d/cuda-repository-pin-600 \
&& sudo apt-key adv --fetch-keys https://developer.download.nvidia.com/
compute/cuda/repos/ubuntu2004/x86_64/3bf863cc.pub \
```

```
&& sudo add-apt-repository 'deb http://developer.download.nvidia.com/compute/
cuda/repos/ubuntu2004/x86_64/ /' \
&& sudo apt update \
&& sudo apt install nvidia-dkms-535 \
&& sudo apt install -o Dpkg::Options::='--force-overwrite' cuda-drivers-535
 cuda-toolkit-12-3 libcudnn8 libcudnn8-dev -y
```

- `p4d.24xlarge` y `p5.48xlarge`

```
$ sudo apt-key adv --fetch-keys http://developer.download.nvidia.com/compute/
machine-learning/repos/ubuntu2004/x86_64/7fa2af80.pub \
&& wget -O /tmp/deeplearning.deb http://developer.download.nvidia.com/compute/
machine-learning/repos/ubuntu2004/x86_64/nvidia-machine-learning-repo-
ubuntu2004_1.0.0-1_amd64.deb \
&& sudo dpkg -i /tmp/deeplearning.deb \
&& wget -O /tmp/cuda.pin https://developer.download.nvidia.com/compute/cuda/
repos/ubuntu2004/x86_64/cuda-ubuntu2004.pin \
&& sudo mv /tmp/cuda.pin /etc/apt/preferences.d/cuda-repository-pin-600 \
&& sudo apt-key adv --fetch-keys https://developer.download.nvidia.com/
compute/cuda/repos/ubuntu2004/x86_64/3bf863cc.pub \
&& sudo add-apt-repository 'deb http://developer.download.nvidia.com/compute/
cuda/repos/ubuntu2004/x86_64/ /' \
&& sudo apt update \
&& sudo apt install nvidia-kernel-open-535 \
&& sudo apt install -o Dpkg::Options::='--force-overwrite' cuda-drivers-535
 cuda-toolkit-12-3 libcudnn8 libcudnn8-dev -y
```

6. Reinicie la instancia y vuelva a conectarse a ella.
7. (Solo para `p4d.24xlarge` y `p5.48xlarge`) Instale Nvidia Fabric Manager.

   a. Debe instalar la versión de Nvidia Fabric Manager que coincida con la versión del módulo del kernel de Nvidia que instaló en el paso anterior.

      Ejecute el siguiente comando para determinar la versión del módulo del kernel de Nvidia.

      ```
      $ cat /proc/driver/nvidia/version | grep "Kernel Module"
      ```

      A continuación, se muestra un ejemplo del resultado.

      ```
      NVRM version: NVIDIA UNIX x86_64 Kernel Module  450.42.01  Tue Jun 15
       21:26:37 UTC 2021
      ```

En el ejemplo anterior, la versión principal `450` del módulo del kernel. Esto significa que necesita instalar la versión `450` de Nvidia Fabric Manager.

b. Instale Nvidia Fabric Manager. Ejecute el siguiente comando y especifique la versión principal identificada en el paso anterior.

```
$ sudo apt install -o Dpkg::Options::='--force-overwrite' nvidia-
fabricmanager-major_version_number
```

Por ejemplo, si se instaló la versión principal `450` del módulo de kernel, utilice el siguiente comando para instalar la versión correspondiente de Nvidia Fabric Manager.

```
$ sudo apt install -o Dpkg::Options::='--force-overwrite' nvidia-
fabricmanager-450
```

c. Inicie el servicio y asegúrese de que se inicie de forma automática cuando se inicia la instancia. Nvidia Fabric Manager es necesario para la administración de NV Switch.

```
$ sudo systemctl start nvidia-fabricmanager && sudo systemctl enable nvidia-
fabricmanager
```

8. Asegúrese de que las rutas CUDA se establecen cada vez que se inicia la instancia.

   - Para intérpretes de comandos bash, agregue las siguientes instrucciones a `/home/username/.bashrc` y `/home/username/.bash_profile`.

   ```
   export PATH=/usr/local/cuda/bin:$PATH
   export LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
   lib64:$LD_LIBRARY_PATH
   ```

   - Para intérpretes de comandos tcsh, agregue las siguientes instrucciones a `/home/username/.cshrc`.

   ```
   setenv PATH=/usr/local/cuda/bin:$PATH
   setenv LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
   lib64:$LD_LIBRARY_PATH
   ```

9. Para confirmar que los controladores de la GPU Nvidia son funcionales, ejecute el siguiente comando.

```
$ nvidia-smi -q | head
```

El comando debe devolver información sobre las GPU de Nvidia, los controladores de GPU de Nvidia y el kit de herramientas Nvidia CUDA.

Paso 4: instalación de GDRCopy

Instale GDRCopy para mejorar el rendimiento de Libfabric. Para obtener más información sobre GDRCopy, consulte el repositorio de GDRCopy.

Amazon Linux 2, CentOS 7, RHEL 7/8/9, and Rocky Linux 8/9

Para instalar GDRCopy

1. Instale las dependencias requeridas.

```
$ sudo yum -y install dkms rpm-build make check check-devel subunit subunit-
devel
```

2. Descargue y extraiga el paquete de GDRCopy.

```
$ wget https://github.com/NVIDIA/gdrcopy/archive/refs/tags/v2.4.tar.gz \
&& tar xf v2.4.tar.gz ; cd gdrcopy-2.4/packages
```

3. Compile el paquete RPM de GDRCopy.

```
$ CUDA=/usr/local/cuda ./build-rpm-packages.sh
```

4. Instale el paquete RPM de GDRCopy.

```
$ sudo rpm -Uvh gdrcopy-kmod-2.4-1dkms.noarch*.rpm \
&& sudo rpm -Uvh gdrcopy-2.4-1.x86_64*.rpm \
&& sudo rpm -Uvh gdrcopy-devel-2.4-1.noarch*.rpm
```

Ubuntu 20.04/22.04

Para instalar GDRCopy

1. Instale las dependencias requeridas.

```
$ sudo apt -y install build-essential devscripts debhelper check libsubunit-dev
 fakeroot pkg-config dkms
```

2. Descargue y extraiga el paquete de GDRCopy.

```
$ wget https://github.com/NVIDIA/gdrcopy/archive/refs/tags/v2.4.tar.gz \
&& tar xf v2.4.tar.gz \
&& cd gdrcopy-2.4/packages
```

3. Compile el paquete RPM de GDRCopy.

```
$ CUDA=/usr/local/cuda ./build-deb-packages.sh
```

4. Instale el paquete RPM de GDRCopy.

```
$ sudo dpkg -i gdrdrv-dkms_2.4-1_amd64.*.deb \
&& sudo dpkg -i libgdrapi_2.4-1_amd64.*.deb \
&& sudo dpkg -i gdrcopy-tests_2.4-1_amd64.*.deb \
&& sudo dpkg -i gdrcopy_2.4-1_amd64.*.deb
```

Paso 5: instalación del software EFA

Instale el kernel habilitado para EFA, los controladores de EFA, Libfabric y la pila Open MPI necesarios para admitir EFA en su instancia temporal.

Para instalar el software EFA

1. Conéctese a la instancia que lanzó. Para obtener más información, consulte Conexión con la instancia de Linux.
2. Descargue los archivos de instalación de software de EFA. Los archivos de instalación de software están empaquetados en un archivo tarball comprimido (`.tar.gz`). Para descargar la última versión estable, utilice el comando siguiente.

   ```
   $ C:\> curl -O https://efa-installer.amazonaws.com/aws-efa-installer-1.32.0.tar.gz
   ```

   También puede obtener la última versión reemplazando el número de versión por `latest` en el comando anterior.
3. (Opcional) Verifique la autenticidad y la integridad del archivo tarball (`.tar.gz`) de EFA.

Le recomendamos que lo haga para verificar la identidad del editor de software y para verificar que el archivo no se haya modificado ni dañado desde que se publicó. Si no desea verificar el archivo tarball, omita este paso.

> **Note**
>
> De forma alternativa, si prefiere verificar el archivo tarball con una suma de comprobación MD5 o SHA256, consulte Verificar el instalador de EFA mediante una suma de comprobación.

a. Descargue la clave pública de GPG e impórtela a su conjunto de claves.

```
$ wget https://efa-installer.amazonaws.com/aws-efa-installer.key && gpg --
import aws-efa-installer.key
```

El comando debe devolver un valor de clave. Anote el valor de clave, ya que lo necesitará en el siguiente paso.

b. Verifique la huella digital de la clave de GPG. Ejecute el siguiente comando y especifique el valor de clave del paso anterior.

```
$ gpg --fingerprint key_value
```

El comando debe devolver una huella digital idéntica a `4E90 91BC BB97 A96B 26B1 5E59 A054 80B1 DD2D 3CCC`. Si la huella digital no coincide, no ejecute el script de instalación de EFA y contáctese con AWS Support.

c. Descargue el archivo de firma y verifique la firma del archivo tarball de EFA.

```
$ wget https://efa-installer.amazonaws.com/aws-efa-installer-1.32.0.tar.gz.sig
 && gpg --verify ./aws-efa-installer-1.32.0.tar.gz.sig
```

A continuación se muestra un ejemplo de salida.

```
gpg: Signature made Wed 29 Jul 2020 12:50:13 AM UTC using RSA key ID DD2D3CCC
gpg: Good signature from "Amazon EC2 EFA <ec2-efa-maintainers@amazon.com>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
```

```
Primary key fingerprint: 4E90 91BC BB97 A96B 26B1  5E59 A054 80B1 DD2D 3CCC
```

Si el resultado incluye `Good signature` y la huella digital coincide con la huella digital del paso anterior, avance al siguiente paso. Si no es así, no ejecute el script de instalación de EFA y contáctese con AWS Support.

4. Extraiga los archivos desde el archivo `.tar.gz` comprimido y acceda al directorio extraído.

```
$ C:\> tar -xf aws-efa-installer-1.32.0.tar.gz && cd aws-efa-installer
```

5. Ejecute el script de instalación de software de EFA.

> **Note**
>
> A partir de la versión 1.30.0 de EFA, tanto Open MPI 4 como Open MPI 5 se instalan de forma predeterminada. A menos que necesite Open MPI 5, le recomendamos que instale únicamente Open MPI 4. El siguiente comando solo instala Open MPI 4. Si desea instalar Open MPI 4 y Open MPI 5, quite `--mpi=openmpi4`.

```
$ C:\> sudo ./efa_installer.sh -y --mpi=openmpi4
```

Libfabric está instalado en el directorio `/opt/amazon/efa`, mientras que Open MPI está instalado en el directorio `/opt/amazon/openmpi`.

6. Si el instalador de EFA le pide que reinicie la instancia, hágalo y vuelva a conectarse a la instancia. De lo contrario, cierre la sesión de la instancia y vuelva a iniciar sesión para completar la instalación.
7. Confirme que los componentes de software de EFA se han instalado correctamente.

```
$ C:\> fi_info -p efa -t FI_EP_RDM
```

El comando debe devolver información acerca de las interfaces de EFA de Libfabric. En el siguiente ejemplo, se muestra el comando de salida.

- `p3dn.24xlarge` con interfaz de red única

```
provider: efa
fabric: EFA-fe80::94:3dff:fe89:1b70
```

```
domain: efa_0-rdm
version: 2.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
```

- `p4d.24xlarge` y `p5.48xlarge` con múltiples interfaces de red

```
provider: efa
fabric: EFA-fe80::c6e:8fff:fef6:e7ff
domain: efa_0-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
provider: efa
fabric: EFA-fe80::c34:3eff:feb2:3c35
domain: efa_1-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
provider: efa
fabric: EFA-fe80::c0f:7bff:fe68:a775
domain: efa_2-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
provider: efa
fabric: EFA-fe80::ca7:b0ff:fea6:5e99
domain: efa_3-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
```

Paso 6: instalar NCCL

Instale NCCL. Para obtener más información sobre NCCL, consulte el repositorio de NCCL.

Para instalar NCCL

1. Vaya al directorio `/opt`.

```
$ cd /opt
```

2. Clone el repositorio oficial de NCCL en la instancia y vaya al repositorio clonado local.

```
$ sudo git clone https://github.com/NVIDIA/nccl.git && cd nccl
```

3. Cree e instale NCCL y especifique el directorio de instalación de CUDA.

```
$ sudo make -j src.build CUDA_HOME=/usr/local/cuda
```

Paso 7: instalar el complemento aws-ofi-nccl

El complemento aws-ofi-nccl asigna las API de transporte orientadas a la conexión de NCCL a la interfaz de confianza sin conexión de libfabric. Esto le permite utilizar Libfabric como proveedor de red mientras ejecuta aplicaciones basadas en NCCL. Para obtener más información sobre el complemento aws-ofi-nccl, consulte el repositorio de aws-ofi-nccl.

Para instalar el complemento aws-ofi-nccl

1. Vaya al directorio de inicio.

```
$ cd $HOME
```

2. (Solo para Amazon Linux 2 y Ubuntu) Instale las utilidades necesarias.

   - Amazon Linux 2

   ```
   $ sudo yum install hwloc-devel
   ```

   - Ubuntu 20.04

   ```
   $ sudo apt-get install libhwloc-dev
   ```

3. Descargue los archivos del complemento aws-ofi-nccl. Los archivos están empaquetados en un archivo tarball comprimido (`.tar.gz`).

```
$ wget https://github.com/aws/aws-ofi-nccl/releases/download/v1.9.1-aws/aws-ofi-
nccl-1.9.1-aws.tar.gz
```

4. Extraiga los archivos desde el archivo .tar.gz comprimido y acceda al directorio extraído.

```
$ tar -xf aws-ofi-nccl-1.9.1-aws.tar.gz && cd aws-ofi-nccl-1.9.1-aws
```

5. Para generar los archivos make, ejecute el script `configure` y especifique los directorios de instalación de MPI, Libfabric, NCCL y CUDA.

```
$ ./configure --prefix=/opt/aws-ofi-nccl --with-mpi=/opt/amazon/openmpi \
--with-libfabric=/opt/amazon/efa \
--with-cuda=/usr/local/cuda \
--enable-platform-aws
```

6. Agregue el directorio Open MPI a la variable `PATH`.

```
$ export PATH=/opt/amazon/openmpi/bin/:$PATH
```

7. Instale el complemento aws-ofi-nccl.

```
$ make && sudo make install
```

Paso 8: instalar las pruebas de NCCL

Instale las pruebas de NCCL. Las pruebas de NCCL le permiten confirmar que NCCL está instalado correctamente y que está funcionando como se esperaba. Para obtener más información sobre las pruebas de NCCL, consulte el repositorio nccl-tests.

Para instalar las pruebas de NCCL

1. Vaya al directorio de inicio.

```
$ cd $HOME
```

2. Clone el repositorio oficial nccl-tests en la instancia y vaya al repositorio clonado local.

```
$ git clone https://github.com/NVIDIA/nccl-tests.git && cd nccl-tests
```

3. Añada el directorio Libfabric a la variable `LD_LIBRARY_PATH`.

   - Amazon Linux, Amazon Linux 2, RHEL, Rocky Linux 8/9 y CentOS

```
$ export LD_LIBRARY_PATH=/opt/amazon/efa/lib64:$LD_LIBRARY_PATH
```

   - Ubuntu

```
$ export LD_LIBRARY_PATH=/opt/amazon/efa/lib:$LD_LIBRARY_PATH
```

4. Instale las pruebas NCCL y especifique los directorios de instalación MPI, NCCL y CUDA.

```
$ make MPI=1 MPI_HOME=/opt/amazon/openmpi NCCL_HOME=/opt/nccl/build CUDA_HOME=/usr/
local/cuda
```

Paso 9: prueba de la configuración de EFA y NCCL

Ejecute una prueba para asegurarse de que su instancia temporal esté configurada correctamente para EFA y NCCL.

Para probar la configuración de EFA y NCCL

1. Cree un archivo de hosts que especifique los hosts en los que desea ejecutar las pruebas. El siguiente comando crea un archivo de hosts con el nombre `my-hosts` que incluye una referencia a la propia instancia.

   IMDSv2

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
    "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/
   meta-data/local-ipv4 >> my-hosts
   ```

   IMDSv1

   ```
   [ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/local-ipv4 >> my-
   hosts
   ```

2. Ejecute la prueba y especifique el archivo de hosts (`--hostfile`) y el número de GPUs que desea usar (`-n`). El siguiente comando ejecuta la prueba `all_reduce_perf` en 8 GPUs de la propia instancia y especifica las siguientes variables de entorno.

   - `FI_EFA_USE_DEVICE_RDMA=1`: (solo `p4d.24xlarge`) utiliza la funcionalidad de RDMA del dispositivo para la transferencia de un solo lado y de dos lados.

- `NCCL_DEBUG=INFO`: habilita la salida de depuración detallada. También puede especificar `VERSION` para imprimir solo la versión de NCCL al inicio de la prueba o `WARN` para recibir solo mensajes de error.

Para obtener más información sobre los argumentos de prueba de NCCL, consulte el archivo README de pruebas de NCCL en el reposorio nccl-tests oficial.

- `p3dn.24xlarge`

```
$ /opt/amazon/openmpi/bin/mpirun \
    -x LD_LIBRARY_PATH=/opt/nccl/build/lib:/usr/local/cuda/lib64:/opt/amazon/efa/
lib:/opt/amazon/openmpi/lib:/opt/aws-ofi-nccl/lib:$LD_LIBRARY_PATH \
    -x NCCL_DEBUG=INFO \
    --hostfile my-hosts -n 8 -N 8 \
    --mca pml ^cm --mca btl tcp,self --mca btl_tcp_if_exclude lo,docker0 --bind-
to none \
    $HOME/nccl-tests/build/all_reduce_perf -b 8 -e 1G -f 2 -g 1 -c 1 -n 100
```

- `p4d.24xlarge` y `p5.48xlarge`

```
$ /opt/amazon/openmpi/bin/mpirun \
    -x FI_EFA_USE_DEVICE_RDMA=1 \
    -x LD_LIBRARY_PATH=/opt/nccl/build/lib:/usr/local/cuda/lib64:/opt/amazon/efa/
lib:/opt/amazon/openmpi/lib:/opt/aws-ofi-nccl/lib:$LD_LIBRARY_PATH \
    -x NCCL_DEBUG=INFO \
    --hostfile my-hosts -n 8 -N 8 \
    --mca pml ^cm --mca btl tcp,self --mca btl_tcp_if_exclude lo,docker0 --bind-
to none \
    $HOME/nccl-tests/build/all_reduce_perf -b 8 -e 1G -f 2 -g 1 -c 1 -n 100
```

3. Puede confirmar que EFA está activo como proveedor subyacente de NCCL cuando se imprime el registro `NCCL_DEBUG`.

```
ip-192-168-2-54:14:14 [0] NCCL INFO NET/OFI Selected Provider is efa*
```

La siguiente información adicional se muestra cuando se utiliza una instancia `p4d.24xlarge`.

```
ip-192-168-2-54:14:14 [0] NCCL INFO NET/OFI Running on P4d platform, Setting
 NCCL_TOPO_FILE environment variable to /home/ec2-user/install/plugin/share/aws-
ofi-nccl/xml/p4d-24xl-topo.xml
```

Paso 10: instalar las aplicaciones de machine learning

Instale la aplicación de machine learning en la instancia temporal. El procedimiento de instalación varía en función de la aplicación de machine learning específica. Para obtener más información sobre la instalación de software en la instancia de Linux, consulte Manage software on your Amazon Linux 2 instance.

> **Note**
>
> Consulte la documentación de su aplicación de machine learning para ver las instrucciones de instalación.

Paso 11: creación de una AMI habilitada para EFA y NCCL

Después de haber instalado los componentes de software requeridos, crea una AMI que puede reutilizar para iniciar las instancias habilitadas para EFA.

Para crear una AMI desde la instancia temporal

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancias).
3. Seleccione la instancia temporal que creó y elija Acciones, Imagen, Crear imagen.
4. En Crear imagen, realice lo siguiente:
   a. En Nombre de imagen, ingrese un nombre descriptivo para la AMI.
   b. (Opcional) En Descripción de imagen, ingrese una breve descripción del propósito la AMI.
   c. Elija Crear imagen.
5. En el panel de navegación, elija AMI.
6. Localice la AMI que creó en la lista. Espere a que el estado pase de `pending` a `available` antes de continuar con el paso siguiente.

Paso 12: terminar la instancia temporal

En este punto, ya no necesita la instancia temporal que lanzó. Puede terminar la instancia para dejar de incurrir en cargos debido a esta.

Para terminar la instancia temporal

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancias).
3. Seleccione la instancia temporal que creó y, a continuación, elija Acciones, Estado de instancia, Terminar instancia.
4. Cuando se le indique que confirme, elija Terminar.

Paso 13: inicialización de instancias habilitadas para EFA en un grupo con ubicación en clúster

Lance las instancias habilitadas para EFA y NCCL en un grupo de ubicación en clúster utilizando la AMI habilitada para EFA y el grupo de seguridad habilitado para EFA que creó anteriormente.

> **Note**
>
> - No es un requisito absoluto lanzar las instancias habilitadas con un EFA a un grupo de ubicación de clústeres. Sin embargo, le recomendamos ejecutar sus instancias habilitadas para EFA en un grupo con ubicación en clúster a medida que inicia las instancias en un grupo de baja latencia en una única zona de disponibilidad.
> - Para garantizar que la capacidad esté disponible a medida que escala las instancias del clúster, puede crear una reserva de capacidad para su grupo con ubicación en clúster. Para obtener más información, consulte Las reservas de capacidad en grupos con ubicación en clúster.

New console

Para iniciar una instancia temporal

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instancias y, a continuación, Iniciar instancias para abrir el nuevo asistente de inicialización de instancias.
3. (Opcional) En la sección Nombre y etiquetas, proporcione un nombre para la instancia, como `EFA-instance`. El nombre se asigna a la instancia como etiqueta de recurso (`Name=`*`EFA-instance`*).

4. En la sección Imágenes de aplicaciones y sistema operativo, elija Mi AMI y, a continuación, seleccione la AMI que creó en el paso anterior.
5. En la sección Tipo de instancia, seleccione `p3dn.24xlarge` o `p4d.24xlarge`.
6. En la sección Par de claves, seleccione el par de claves que desea utilizar en la instancia.
7. En la sección Configuración de red, elija Editar y realice lo siguiente:
   a. En Subred, elija la subred en la que desea iniciar la instancia. Si no selecciona una subred, no puede habilitar la instancia para EFA.
   b. En Firewall (grupos de seguridad), elija Seleccionar grupo de seguridad existente y, a continuación, seleccione el grupo de seguridad que creó en el paso anterior.
   c. Expanda la sección Advanced network configuration (Configuración avanzada de la red) y en Elastic Fabric Adapter, seleccione Enable (Habilitar).
8. (Opcional) En la sección Storage (Almacenamiento), configure los volúmenes según sea necesario.
9. En la sección Detalles avanzados, para Nombre del grupo de ubicación, seleccione el grupo con ubicación en clúster en el que se iniciará la instancia. Si necesita crear un nuevo grupo con ubicación en clúster, elija Create new placement group (Crear nuevo grupo de ubicación).
10. En el panel Summary (Resumen) que se encuentra a la derecha, en Number of instances (Cantidad de instancias), ingrese la cantidad de instancias habilitadas para EFA que desea lanzar y, a continuación, elija Launch instance (Lanzar instancia).

Old console

Para iniciar las instancias habilitadas para EFA y NCCL en un grupo con ubicación en clúster

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. Elija Iniciar instancia.
3. En la página Elegir una AMI, elija Mi AMI, encuentre la AMI que creó anteriormente y, a continuación, elija Seleccionar.
4. En la página Elegir un tipo de instancia, seleccione p3dn.24xlarge y, a continuación, elija Siguiente: Configurar detalles de instancia.
5. En la página Configurar detalles de instancia, haga lo siguiente:

a. En Número de instancias, ingrese el número de instancias habilitadas para EFA y NCCL que desea iniciar.

b. En Red y Subred, seleccione la VPC y la subred en la que iniciar las instancias.

c. En Grupo de ubicación, seleccione Añadir instancia a grupo de ubicación.

d. En Nombre de grupo de ubicación, seleccione Agregar a un nuevo grupo de ubicación y, a continuación, ingrese un nombre descriptivo para el grupo de ubicación. Luego, en Estrategia de grupo de ubicación, seleccione clúster.

e. En EFA, elija Habilitar.

f. En la sección Interfaces de red, para el dispositivo eth0, elija Nueva interfaz de red. Como opción, puede especificar una dirección IPv4 principal y una o varias direcciones IPv4 secundarias. Si está iniciando la instancia en una subred que tiene un bloque de CIDR de IPv6 asociado, como opción puede especificar una dirección IPv6 principal y una o varias direcciones IPv6 secundarias.

g. Elija Siguiente: Añadir almacenamiento.

6. En la página Agregar almacenamiento, especifique los volúmenes que desea adjuntar a las instancias además de los volúmenes especificados por la AMI (como el volumen de dispositivo raíz). A continuación, elija Siguiente: Agregar etiquetas.
7. En la página Añadir etiquetas, especifique etiquetas para las instancias, por ejemplo, un nombre fácil de recordar, y, a continuación, elija Siguiente: Configurar grupo de seguridad.
8. En la página Configurar grupo de seguridad, en Asignar un grupo de seguridad, seleccione Seleccionar un grupo de seguridad existente y, a continuación, seleccione el grupo de seguridad que creó anteriormente.
9. Elija Review and Launch (Revisar y lanzar).
10. En la página Review Instance Launch (Revisar inicialización de instancia), revise la configuración y, a continuación, elija Launch (iniciar) para elegir un par de claves y iniciar las instancias.

Paso 14: habilitar SSH sin contraseña

Para permitir que las aplicaciones se ejecuten en todas las instancias del clúster, debe habilitar el acceso mediante SSH sin contraseña desde el nodo principal hasta los nodos miembro. El nodo principal es la instancia desde la que se ejecutan las aplicaciones. Las instancias restantes del clúster son los nodos miembros.

Para habilitar SSH sin contraseña entre las instancias del clúster

1. Seleccione una instancia del clúster como nodo principal y conéctese a ella.
2. Desactive `strictHostKeyChecking` y habilite `ForwardAgent` en el nodo principal. Abra `~/.ssh/config` con su editor de texto preferido y agregue lo siguiente.

   ```
   Host *
       ForwardAgent yes
   Host *
       StrictHostKeyChecking no
   ```

3. Genere un par de claves de RSA.

   ```
   $ ssh-keygen -t rsa -N "" -f ~/.ssh/id_rsa
   ```

   El par de claves se crea en el directorio `$HOME/.ssh/`.
4. Cambie los permisos de la clave privada en el nodo principal.

   ```
   $ chmod 600 ~/.ssh/id_rsa
   chmod 600 ~/.ssh/config
   ```

5. Abra `~/.ssh/id_rsa.pub` con su editor de texto preferido y copie la clave.
6. Para cada nodo miembro del clúster, realice lo siguiente:

   a. Conéctese a la instancia.

   b. Abra `~/.ssh/authorized_keys` con su editor de texto preferido y agregue la clave pública que copió anteriormente.
7. Para probar que SSH sin contraseña funciona como se esperaba, conecte al nodo principal y ejecute el siguiente comando.

   ```
   $ ssh member_node_private_ip
   ```

   Debe conectarse al nodo miembro sin que se le pida una clave o una contraseña.

Utilizar una AMI de aprendizaje profundo de AWS

Los siguientes pasos lo ayudan a comenzar con una de las siguientes AMI de aprendizaje profundo de AWS:

- AMI de Deep Learning (Amazon Linux 2)
- AMI de Deep Learning (Ubuntu 20.04)

Para obtener más información, consulte la Guía del usuario de AWS Deep Learning AMI.

> **Note**
>
> Solo se admiten los tipos de instancia `p3dn.24xlarge` y `p4d.24xlarge`.

Contenido

Paso 1: preparar un grupo de seguridad habilitado para EFA

Un EFA requiere un grupo de seguridad que permita todo el tráfico entrante y saliente hacia y desde el propio grupo de seguridad. En el siguiente procedimiento, se crea un grupo de seguridad que permite todo el tráfico entrante y saliente de sí mismo, y que permite el tráfico SSH entrante desde cualquier dirección IPv4 para la conectividad SSH.

> **Important**
>
> Este grupo de seguridad está pensado solo con fines de prueba. Para sus entornos de producción, le recomendamos que cree una regla SSH entrante que permita el tráfico únicamente desde la dirección IP desde la que se conecta, como la dirección IP de su equipo o un rango de direcciones IP en la red local.

Para ver otros escenarios, consulte Reglas de grupo de seguridad para diferentes casos de uso.

Para crear un grupo de seguridad habilitado para EFA

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Grupos de seguridad y, a continuación, elija Crear grupo de seguridad.
3. En la ventana Crear grupo de seguridad, haga lo siguiente:
   a. En Nombre del grupo de seguridad, ingrese un nombre descriptivo para el grupo de seguridad, como, por ejemplo, `EFA-enabled security group`.
   b. (Opcional) En Descripción, ingrese una breve descripción del grupo de seguridad.
   c. En VPC, seleccione la VPC en la que desea iniciar sus instancias habilitadas para EFA.
   d. Elija Crear grupo de seguridad.
4. Seleccione el grupo de seguridad que creó y, en la pestaña Detalles, copie el ID del grupo de seguridad.
5. Con el grupo de seguridad todavía seleccionado, elija Acciones, Editar reglas de entrada y, luego, haga lo siguiente:
   a. Seleccione Agregar regla.
   b. En Tipo, seleccione Todo el tráfico.
   c. En Tipo de origen, elija Personalizar y pegue el ID del grupo de seguridad que copió en el campo.
   d. Seleccione Agregar regla.
   e. En Tipo, seleccione SSH.
   f. En Tipo de origen, elija Cualquiera de IPv4.
   g. Seleccione Guardar reglas.
6. Con el grupo de seguridad todavía seleccionado, elija Acciones, Editar reglas de salida y, luego, haga lo siguiente:
   a. Seleccione Agregar regla.
   b. En Tipo, seleccione Todo el tráfico.
   c. En Tipo de destino, elija Personalizar y pegue el ID del grupo de seguridad que copió en el campo.
   d. Seleccione Guardar reglas.

Paso 2: iniciar una instancia temporal

Lance una instancia temporal que puede utilizar para instalar y configurar los componentes de software de EFA. Puede utilizar esta instancia para crear una AMI habilitada para EFA desde la que puede iniciar sus instancias habilitadas para EFA.

Para iniciar una instancia temporal

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instancias y, a continuación, Iniciar instancias para abrir el nuevo asistente de inicialización de instancias.
3. (Opcional) En la sección Nombre y etiquetas, proporcione un nombre para la instancia, como `EFA-instance`. El nombre se asigna a la instancia como etiqueta de recurso (`Name=`*`EFA-instance`*).
4. En la sección Imágenes de aplicaciones y sistema operativo, seleccione una AMI de aprendizaje profundo de AWS, versión 25.0 o posterior compatible.
5. En la sección Instance type (Tipo de instancia), seleccione `p3dn.24xlarge` o `p4d.24xlarge`.
6. En la sección Par de claves, seleccione el par de claves que desea utilizar en la instancia.
7. En la sección Configuración de red, elija Editar y realice lo siguiente:
   a. En Subred, elija la subred en la que desea iniciar la instancia. Si no selecciona una subred, no puede habilitar la instancia para EFA.
   b. En Firewall (grupos de seguridad), elija Seleccionar grupo de seguridad existente y, a continuación, seleccione el grupo de seguridad que creó en el paso anterior.
   c. Expanda la sección Configuración avanzada de la red y en Elastic Fabric Adapter, seleccione Habilitar.
8. En la sección Storage (Almacenamiento), configure los volúmenes según sea necesario.

   > **Note**
   >
   > Debe aprovisionar 10 a 20 GiB adicionales de almacenamiento para el conjunto de herramientas CUDA de Nvidia. Si no aprovisiona suficiente almacenamiento, recibirá un error de `insufficient disk space` cuando intente instalar los controladores de Nvidia y el kit de herramientas CUDA.

9. En el panel Resumen que se encuentra a la derecha, elija Iniciar instancia.

Paso 3: probar la configuración de EFA y NCCL

Ejecute una prueba para asegurarse de que su instancia temporal esté configurada correctamente para EFA y NCCL.

Para probar la configuración de EFA y NCCL

1. Cree un archivo de hosts que especifique los hosts en los que desea ejecutar las pruebas. El siguiente comando crea un archivo de hosts con el nombre `my-hosts` que incluye una referencia a la propia instancia.

   IMDSv2

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
    "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/
   meta-data/local-ipv4 >> my-hosts
   ```

   IMDSv1

   ```
   [ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/local-ipv4 >> my-
   hosts
   ```

2. Ejecute la prueba y especifique el archivo de hosts (`--hostfile`) y el número de GPUs que desea usar (`-n`). El siguiente comando ejecuta la prueba `all_reduce_perf` en 8 GPUs de la propia instancia y especifica las siguientes variables de entorno.

   - `FI_EFA_USE_DEVICE_RDMA=1`: (solo `p4d.24xlarge`) utiliza la funcionalidad de RDMA del dispositivo para la transferencia de un solo lado y de dos lados.
   - `NCCL_DEBUG=INFO`: habilita la salida de depuración detallada. También puede especificar `VERSION` para imprimir solo la versión de NCCL al inicio de la prueba o `WARN` para recibir solo mensajes de error.

   Para obtener más información sobre los argumentos de prueba de NCCL, consulte el archivo README de pruebas de NCCL en el reposorio nccl-tests oficial.

   - `p3dn.24xlarge`

   ```
   $ /opt/amazon/openmpi/bin/mpirun \
   ```

```
    -x LD_LIBRARY_PATH=/opt/nccl/build/lib:/usr/local/cuda/lib64:/opt/amazon/efa/
lib:/opt/amazon/openmpi/lib:/opt/aws-ofi-nccl/lib:$LD_LIBRARY_PATH \
    -x NCCL_DEBUG=INFO \
    --hostfile my-hosts -n 8 -N 8 \
    --mca pml ^cm --mca btl tcp,self --mca btl_tcp_if_exclude lo,docker0 --bind-
to none \
    $HOME/nccl-tests/build/all_reduce_perf -b 8 -e 1G -f 2 -g 1 -c 1 -n 100
```

- `p4d.24xlarge`

```
$ /opt/amazon/openmpi/bin/mpirun \
    -x FI_EFA_USE_DEVICE_RDMA=1 \
    -x LD_LIBRARY_PATH=/opt/nccl/build/lib:/usr/local/cuda/lib64:/opt/amazon/efa/
lib:/opt/amazon/openmpi/lib:/opt/aws-ofi-nccl/lib:$LD_LIBRARY_PATH \
    -x NCCL_DEBUG=INFO \
    --hostfile my-hosts -n 8 -N 8 \
    --mca pml ^cm --mca btl tcp,self --mca btl_tcp_if_exclude lo,docker0 --bind-
to none \
    $HOME/nccl-tests/build/all_reduce_perf -b 8 -e 1G -f 2 -g 1 -c 1 -n 100
```

3. Puede confirmar que EFA está activo como proveedor subyacente de NCCL cuando se imprime el registro `NCCL_DEBUG`.

```
ip-192-168-2-54:14:14 [0] NCCL INFO NET/OFI Selected Provider is efa*
```

La siguiente información adicional se muestra cuando se utiliza una instancia `p4d.24xlarge`.

```
ip-192-168-2-54:14:14 [0] NCCL INFO NET/OFI Running on P4d platform, Setting
 NCCL_TOPO_FILE environment variable to /home/ec2-user/install/plugin/share/aws-
ofi-nccl/xml/p4d-24xl-topo.xml
```

Paso 4: instalar las aplicaciones de machine learning

Instale la aplicación de machine learning en la instancia temporal. El procedimiento de instalación varía en función de la aplicación de machine learning específica. Para obtener más información sobre la instalación de software en la instancia de Linux, consulte Manage software on your Amazon Linux 2 instance.

> **Note**
>
> Consulte la documentación de su aplicación de machine learning para ver las instrucciones de instalación.

Paso 5: crear una AMI habilitada para EFA y NCCL

Después de haber instalado los componentes de software requeridos, crea una AMI que puede reutilizar para iniciar las instancias habilitadas para EFA.

Para crear una AMI desde la instancia temporal

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancias).
3. Seleccione la instancia temporal que creó y elija Acciones, Imagen, Crear imagen.
4. En Crear imagen, realice lo siguiente:
   a. En Nombre de imagen, ingrese un nombre descriptivo para la AMI.
   b. (Opcional) En Descripción de imagen, ingrese una breve descripción del propósito la AMI.
   c. Elija Crear imagen.
5. En el panel de navegación, elija AMI.
6. Localice la AMI que creó en la lista. Espere a que el estado pase de `pending` a `available` antes de continuar con el paso siguiente.

Paso 6: terminar la instancia temporal

En este punto, ya no necesita la instancia temporal que lanzó. Puede terminar la instancia para dejar de incurrir en cargos debido a esta.

Para terminar la instancia temporal

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancias).
3. Seleccione la instancia temporal que creó y, a continuación, elija Acciones, Estado de instancia, Terminar instancia.
4. Cuando se le indique que confirme, elija Terminar.

Paso 7: iniciar instancias habilitadas para EFA en un grupo con ubicación en clúster

Lance las instancias habilitadas para EFA y NCCL en un grupo con ubicación en clúster utilizando la AMI habilitada para EFA y el grupo de seguridad habilitado para EFA que creó anteriormente.

> **Note**
>
> - No es un requisito absoluto lanzar las instancias habilitadas con un EFA a un grupo de ubicación de clústeres. Sin embargo, le recomendamos ejecutar sus instancias habilitadas para EFA en un grupo con ubicación en clúster a medida que inicia las instancias en un grupo de baja latencia en una única zona de disponibilidad.
> - Para garantizar que la capacidad esté disponible a medida que escala las instancias del clúster, puede crear una reserva de capacidad para su grupo con ubicación en clúster. Para obtener más información, consulte Las reservas de capacidad en grupos con ubicación en clúster.

New console

Para iniciar una instancia temporal

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instancias y, a continuación, Iniciar instancias para abrir el nuevo asistente de inicialización de instancias.
3. (Opcional) En la sección Nombre y etiquetas, proporcione un nombre para la instancia, como `EFA-instance`. El nombre se asigna a la instancia como etiqueta de recurso (`Name=`*`EFA-instance`*).
4. En la sección Imágenes de aplicaciones y sistema operativo, elija Mi AMI y, a continuación, seleccione la AMI que creó en el paso anterior.
5. En la sección Tipo de instancia, seleccione `p3dn.24xlarge` o `p4d.24xlarge`.
6. En la sección Par de claves, seleccione el par de claves que desea utilizar en la instancia.
7. En la sección Configuración de red, elija Editar y realice lo siguiente:

   a. En Subred, elija la subred en la que desea iniciar la instancia. Si no selecciona una subred, no puede habilitar la instancia para EFA.

b. En Firewall (grupos de seguridad), elija Seleccionar grupo de seguridad existente y, a continuación, seleccione el grupo de seguridad que creó en el paso anterior.

c. Expanda la sección Advanced network configuration (Configuración avanzada de la red) y en Elastic Fabric Adapter, seleccione Enable (Habilitar).

8. (Opcional) En la sección Storage (Almacenamiento), configure los volúmenes según sea necesario.

9. En la sección Detalles avanzados, para Nombre del grupo de ubicación, seleccione el grupo con ubicación en clúster en el que se iniciará la instancia. Si necesita crear un nuevo grupo con ubicación en clúster, elija Create new placement group (Crear nuevo grupo de ubicación).

10. En el panel Summary (Resumen) que se encuentra a la derecha, en Number of instances (Cantidad de instancias), ingrese la cantidad de instancias habilitadas para EFA que desea lanzar y, a continuación, elija Launch instance (Lanzar instancia).

Old console

Para iniciar las instancias habilitadas para EFA y NCCL en un grupo con ubicación en clúster

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

2. Elija Iniciar instancia.

3. En la página Elegir una AMI, elija Mi AMI, encuentre la AMI que creó anteriormente y, a continuación, elija Seleccionar.

4. En la página Elegir un tipo de instancia, seleccione p3dn.24xlarge y, a continuación, elija Siguiente: Configurar detalles de instancia.

5. En la página Configurar detalles de instancia, haga lo siguiente:

a. En Número de instancias, ingrese el número de instancias habilitadas para EFA y NCCL que desea iniciar.

b. En Red y Subred, seleccione la VPC y la subred en la que iniciar las instancias.

c. En Grupo de ubicación, seleccione Añadir instancia a grupo de ubicación.

d. En Nombre de grupo de ubicación, seleccione Agregar a un nuevo grupo de ubicación y, a continuación, ingrese un nombre descriptivo para el grupo de ubicación. Luego, en Estrategia de grupo de ubicación, seleccione clúster.

e. En EFA, elija Habilitar.

f. En la sección Interfaces de red, para el dispositivo eth0, elija Nueva interfaz de red. Como opción, puede especificar una dirección IPv4 principal y una o varias direcciones IPv4 secundarias. Si está iniciando la instancia en una subred que tiene un bloque de CIDR de IPv6 asociado, como opción puede especificar una dirección IPv6 principal y una o varias direcciones IPv6 secundarias.

g. Elija Siguiente: Añadir almacenamiento.

6. En la página Agregar almacenamiento, especifique los volúmenes que desea adjuntar a las instancias además de los volúmenes especificados por la AMI (como el volumen de dispositivo raíz). A continuación, elija Siguiente: Agregar etiquetas.
7. En la página Añadir etiquetas, especifique etiquetas para las instancias, por ejemplo, un nombre fácil de recordar, y, a continuación, elija Siguiente: Configurar grupo de seguridad.
8. En la página Configurar grupo de seguridad, en Asignar un grupo de seguridad, seleccione Seleccionar un grupo de seguridad existente y, a continuación, seleccione el grupo de seguridad que creó anteriormente.
9. Elija Review and Launch (Revisar y lanzar).
10. En la página Revisar inicialización de instancia, revise la configuración y, a continuación, elija Iniciar para elegir un par de claves e iniciar las instancias.

Paso 8: habilitar SSH sin contraseña

Para permitir que las aplicaciones se ejecuten en todas las instancias del clúster, debe habilitar el acceso mediante SSH sin contraseña desde el nodo principal hasta los nodos miembro. El nodo principal es la instancia desde la que se ejecutan las aplicaciones. Las instancias restantes del clúster son los nodos miembros.

Para habilitar SSH sin contraseña entre las instancias del clúster

1. Seleccione una instancia del clúster como nodo principal y conéctese a ella.
2. Desactive `strictHostKeyChecking` y habilite `ForwardAgent` en el nodo principal. Abra `~/.ssh/config` con su editor de texto preferido y agregue lo siguiente.

```
Host *
    ForwardAgent yes
Host *
    StrictHostKeyChecking no
```

3. Genere un par de claves de RSA.

```
$ ssh-keygen -t rsa -N "" -f ~/.ssh/id_rsa
```

El par de claves se crea en el directorio `$HOME/.ssh/`.

4. Cambie los permisos de la clave privada en el nodo principal.

```
$ chmod 600 ~/.ssh/id_rsa
chmod 600 ~/.ssh/config
```

5. Abra `~/.ssh/id_rsa.pub` con su editor de texto preferido y copie la clave.
6. Para cada nodo miembro del clúster, realice lo siguiente:
   a. Conéctese a la instancia.
   b. Abra `~/.ssh/authorized_keys` con su editor de texto preferido y agregue la clave pública que copió anteriormente.
7. Para probar que SSH sin contraseña funciona como se esperaba, conecte al nodo principal y ejecute el siguiente comando.

```
$ ssh member_node_private_ip
```

Debe conectarse al nodo miembro sin que se le pida una clave o una contraseña.

Trabajar con EFA

Puede crear, utilizar y administrar un EFA de modo muy similar a otras interfaces de red elástica en Amazon EC2. Sin embargo, a diferencia de las interfaces de red elástica, los EFAs no se pueden adjuntar o separar de una instancia en estado de ejecución.

Requisitos de EFA

Para utilizar un EFA, debe hacer lo siguiente:

- Elija uno de los tipos de instancia admitidos.
- Utilice una AMI para uno de los sistemas operativos compatibles.
- Instale los componentes de software de EFA. Para obtener más información, consulte Paso 3: instalar el software EFA y Paso 5: (opcional) instalar Intel MPI.

- Utilice un grupo de seguridad que permita todo el tráfico entrante y saliente hacia y desde el propio grupo de seguridad. Para obtener más información, consulte Paso 1: preparar un grupo de seguridad habilitado para EFA.

Contenido

Crear un EFA

Puede crear un EFA en una subred en una VPC. No puede mover el EFA a otra subred después de crearla y solo puede adjuntarlo a instancias detenidas en la misma zona de disponibilidad.

Para crear un nuevo EFA con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Network Interfaces.
3. Elija Crear interfaz de red.
4. En Descripción, escriba un nombre descriptivo para el EFA.
5. En Subred, seleccione la subred en la que crear el EFA.
6. En IP privada, introduzca la dirección IPv4 privada principal. Si no especifica una dirección IPv4, seleccionamos una dirección IPv4 privada disponible desde la subred seleccionada.
7. (IPv6 únicamente) Si ha seleccionado una subred con un bloque de CIDR IPv6 asociado, puede especificar opcionalmente una dirección IPv6 en el campo IP IPv6.
8. En Grupos de seguridad, seleccione uno o varios grupos de seguridad.
9. Para EFA, elija Habilitado.

10. Elija Sí, crear.

Para crear un nuevo EFA con la AWS CLI

Utilice el comando create-network-interface y para `interface-type`, especifique `efa`, como se muestra en el ejemplo siguiente.

```
aws ec2 create-network-interface --subnet-id subnet-01234567890 --
description example_efa --interface-type efa
```

Asociar un EFA a una instancia detenida

Puede adjuntar un EFA a cualquier instancia admitida que esté en el estado `stopped`. No puede adjuntar un EFA a una instancia que esté en el estado `running`. Para obtener más información sobre los tipos de instancia admitidos, consulte Tipos de instancias admitidos.

Puede asociar un EFA a una instancia de la misma manera que asocia una interfaz de red elástica a una instancia. Para obtener más información, consulte Asociar una interfaz de red a una instancia.

Asociar un EFA al iniciar una instancia

Para adjuntar un EFA existente al iniciar una instancia (AWS CLI)

Utilice el comando run-instances y para NetworkInterfaceId, especifique el ID del EFA, como se muestra en el ejemplo siguiente.

```
aws ec2 run-instances --image-id ami_id --count 1 --instance-
type c5n.18xlarge --key-name my_key_pair --network-interfaces
 DeviceIndex=0,NetworkInterfaceId=efa_id,Groups=sg_id,SubnetId=subnet_id
```

Para adjuntar un EFA nuevo al iniciar una instancia (AWS CLI)

Utilice el comando run-instances y para InterfaceType, especifique `efa`, como se muestra en el ejemplo siguiente.

```
aws ec2 run-instances --image-id ami_id --count 1 --instance-
type c5n.18xlarge --key-name my_key_pair --network-interfaces
 DeviceIndex=0,InterfaceType=efa,Groups=sg_id,SubnetId=subnet_id
```

Agregar un EFA a una plantilla de inicialización

Puede crear una plantilla de inicialización que contenga la información de configuración necesaria para iniciar instancias de EFA. Para crear una plantilla de inicialización habilitada para EFA, cree una nueva plantilla de inicialización y especifique un tipo de instancia admitido, la AMI habilitada para EFA y un grupo de seguridad habilitado para EFA. Para obtener más información, consulte Introducción a EFA y MPI.

Puede aprovechar las plantillas de inicialización para iniciar instancias habilitadas para EFA con otros servicios de AWS, como AWS Batch o AWS ParallelCluster.

Para obtener más información acerca de la creación de plantillas de inicialización, consulte Creación de una plantilla de lanzamiento.

Administrar direcciones IP para un EFA

Puede cambiar las direcciones IP asociadas a un EFA. Si tiene una dirección IP elástica, puede asociarla a un EFA. Si su EFA se aprovisiona en una subred que tiene un bloque de CIDR de IPv6 asociado, puede asociar una o varias direcciones IPv6 al EFA.

Asigne una dirección IP elástica (IPv4) e IPv6 a un EFA de la misma manera que asigna una dirección IP a una interfaz de red elástica. Para obtener más información, vea Administración de direcciones IP.

Cambiar el grupo de seguridad de un EFA

Puede cambiar el grupo de seguridad que está asociado a un EFA. Para habilitar la funcionalidad de omisión del sistema operativo, el EFA debe formar parte de un grupo de seguridad que permita todo el tráfico entrante y saliente hacia y desde el propio grupo de seguridad.

Cambie el grupo de seguridad asociado a un EFA de la misma manera que cambia el grupo de seguridad que está asociado a una interfaz de red elástica. Para obtener más información, vea Cambiar el grupo de seguridad.

Separar un EFA

Para separar un EFA de una instancia, primero debe detener la instancia. No puede separar un EFA de una instancia que está en estado de ejecución.

Separe un EFA desde una instancia de la misma manera que separe una interfaz de red elástica de una instancia. Para obtener más información, consulte Desasociar una interfaz de red de una instancia.

Vista de EFAs

Puede ver todos los EFAs en su cuenta.

Los EFAs se ven de la misma manera que las interfaces de red elástica. Para obtener más información, consulte Ver detalles sobre una interfaz de red.

Eliminar un EFA

Para eliminar un EFA, primero debe separarlo de la instancia. No puede eliminar un EFA mientras esté conectado a una instancia.

Los EFAs se eliminan de la misma manera que las interfaces de red elástica. Para obtener más información, consulte Eliminar una interfaz de red.

Monitorear un EFA

Puede utilizar las siguientes características para monitorizar el rendimiento de sus Elastic Fabric Adapters.

Registros de flujo de Amazon VPC

Puede crear un registro de flujo de Amazon VPC para capturar información acerca el tráfico entrante y saliente de un EFA. Los datos del registro de flujo se pueden publicar en Amazon CloudWatch Logs y Amazon S3. Una vez creado un registro de flujo, puede recuperarlo y ver sus datos en el destino elegido. Para obtener más información, consulte Registros de flujo de VPC en la Guía del usuario de Amazon VPC.

Un registro de flujo para un EFA se crea de la misma manera que se crea un registro de flujo para una interfaz de red elástica. Para obtener más información, consulte Creación de un registro de flujo en la Guía del usuario de Amazon VPC.

En las entradas de registro de flujo, el tráfico de EFA se identifica mediante `srcAddress` y `destAddress` que tienen formato de direcciones MAC, tal como se muestra en el ejemplo siguiente.

```
version accountId  eniId       srcAddress       destAddress       sourcePort destPort
 protocol packets bytes start      end        action log-status
```

```
2       3794735123 eni-10000001 01:23:45:67:89:ab 05:23:45:67:89:ab -          -
 -        9       5689  1521232534 1524512343 ACCEPT OK
```

Amazon CloudWatch

Amazon CloudWatch proporciona métricas que le permiten monitorizar sus EFAs en tiempo real. Puede recopilar métricas y realizar un seguimiento de las métricas, crear paneles personalizados y definir alarmas que le advierten o que toman medidas cuando una métrica determinada alcanza el umbral que se especifique. Para obtener más información, consulte Monitorear las instancias con CloudWatch.

Verificar el instalador de EFA mediante una suma de comprobación

Si lo desea, puede verificar el archivo tarball de EFA (archivo .tar.gz) utilizando una suma de comprobación MD5 o SHA256. Le recomendamos que lo haga para verificar la identidad del editor de software y para comprobar que la aplicación no se ha modificado ni dañado desde que se publicó.

Para verificar el tarball

Use la utilidad md5sum para la suma de comprobación MD5 o la utilidad sha256sum para la suma de comprobación SHA256, y especifique el nombre de archivo tarball. Debe ejecutar el comando desde el directorio en el que guardó el archivo tarball.

- MD5

```
$  md5sum tarball_filename.tar.gz
```

- SHA256

```
$  sha256sum tarball_filename.tar.gz
```

Los comandos deben devolver un valor de suma de comprobación en el siguiente formato.

```
checksum_value tarball_filename.tar.gz
```

Compare el valor de suma de comprobación devuelto por el comando con el valor de suma de comprobación proporcionado en la tabla siguiente. Si las sumas de comprobación coinciden, entonces es seguro ejecutar el script de instalación. Si las sumas de comprobación no concuerdan, no ejecute el script de instalación y contacte con AWS Support.

Por ejemplo, el siguiente comando verifica el tarball 1.9.4 de EFA utilizando la suma de comprobación SHA256.

```
$  sha256sum aws-efa-installer-1.9.4.tar.gz
```

```
1009b5182693490d908ef0ed2c1dd4f813cc310a5d2062ce9619c4c12b5a7f14 aws-efa-
installer-1.9.4.tar.gz
```

En la tabla siguiente se muestran las sumas de comprobación de las versiones recientes de EFA.

Versión	Descargar URL	Sumas de comprobación
EFA 1.32.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.32.0.tar.gz	MD5: db8d65cc028d8d08b5a9f2d88881c1b1 SHA256: 5f7233760be57f6fee6de8c09acbfbf59238de848e06048dc54d156ef578fc66
EFA 1.31.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.31.0.tar.gz	MD5: 856352f12bef2ccbadcd75e35aa52aaf SHA256: 943325bd37902a4300ac9e5715163537d56ecb4e7b87b37827c3e547aa1897bf
EFA 1.30.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.30.0.tar.gz	MD5: 31f48e1a47fe93ede8ebd273fb747358 SHA256: 876ab9403e07a0c3c91a1a34685a52eced890ae052df94857f6081c5f6c78a0a
EFA 1.29.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.29.1.tar.gz	MD5: e1872ca815d752c1d7c2b5c175e52a16

Versión	Descargar URL	Sumas de comprobación
		SHA256: 178b263b8c25845b63 dc93b25bcdff5870df 5204ec509af26f43e8 d283488744
EFA 1.29.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.29.0.tar.gz	MD5: 39d06a002154d94cd9 82ed348133f385 SHA256: 836655f87015547e73 3e7d9f7c760e4e2469 7f8bbc261bb5f3560a bd4206bc36
EFA 1.28.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.28.0.tar.gz	MD5: 9dc13b744666582260 5e66febe074035 SHA256: 2e625d2d6d3e073b51 78e8e861891273d896 b66d03cb1a32244fd5 6789f1c435
EFA 1.27.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.27.0.tar.gz	MD5: 98bfb515ea3e8d93f5 54020f3837fa15 SHA256: 1d49a97b0bf8d964d9 1652a79ac851f2550e 33a5bf9d0cf86ec935 7ff6579aa3
EFA 1.26.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.26.1.tar.gz	MD5: 884e74671fdef47255 01f7cd2d451d0c SHA256: c616994c924f54ebfa bfab32b7fe8ac56947 fae00a0ff453d975e2 98d174fc96

Versión	Descargar URL	Sumas de comprobación
EFA 1.26.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.26.0.tar.gz	MD5: f8839f12ff2e3b9ba09ae8a82b30e663 SHA256: bc1abc1f76e97d204d3755d2a9ca307fc423e51c63141f798c2f15be3715aa11
EFA 1.25.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.25.1.tar.gz	MD5: 6d876b894547847a45bb8854d4431f18 SHA256: d2abc553d22b89a4ce92882052c1fa6de450d3a801fe005da718b7d4b9602b06
EFA 1.25.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.25.0.tar.gz	MD5: 1993836ca749596051da04694ea0d00c SHA256: 98b7b26ce031a2d6a93de2297cc71b03af647194866369ca53b60d82d45ad342
EFA 1.24.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.24.1.tar.gz	MD5: 211b249f39d53086f3cb0c07665f4e6f SHA256: 120cfeec233af0955623ac7133b674143329f9561a9a8193e473060f596aec62

Versión	Descargar URL	Sumas de comprobación
EFA 1.24.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.24.0.tar.gz	MD5: 7afe0187951e2dd2c9cc4b572e62f924 SHA256: 878623f819a0d9099d76ecd41cf4f569d4c3aac0c9bb7ba9536347c50b6bf88e
EFA 1.23.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.23.1.tar.gz	MD5: 22491e114b6ee7160a8290145dca0c28 SHA256: 5ca848d8e0ff4d1571cd443c36f8d27c8cdf2a0c97e9068ebf000c303fc40797
EFA 1.23.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.23.0.tar.gz	MD5: 38a6d7c1861f5038dba4e441ca7683ca SHA256: 555d497a60f22e3857fdeb3dfc53aa86d05926023c68c916d15d2dc3df6525bd
EFA 1.22.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.22.1.tar.gz	MD5: 600c0ad7cdbc06e8e846cb763f92901b SHA256: f90f3d5f59c031b9a964466b5401e86fd0429272408f6c207c3f9048254e9665

Versión	Descargar URL	Sumas de comprobación
EFA 1.22.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.22.0.tar.gz	MD5: `8f100c93dc8ab519c2aeb5dab89e98f8` SHA256: `f329e7d54a86a03ea51da6ea9a5b68fb354fbae4a57a02f9592e21fce431dc3a`
EFA 1.21.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.21.0.tar.gz	MD5: `959ccc3a4347461909ec02ed3ba7c372` SHA256: `c64e6ca34ccfc3ebe8e82d08899ae8442b3ef552541cf5429c43d11a04333050`
EFA 1.20.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.20.0.tar.gz	MD5: `7ebfbb8e85f1b94709df4ab3db47913b` SHA256: `aeefd2681ffd5c4c631d1502867db5b831621d6eb85b61fe3ec80df983d1dcf0`
EFA 1.19.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.19.0.tar.gz	MD5: `2fd45324953347ec5518da7e3fefa0ec` SHA256: `99b77821b9e72c8dea015cc92c96193e8db307deee05b91a58094cc331f16709`

Versión	Descargar URL	Sumas de comprobación
EFA 1.18.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.18.0.tar.gz	MD5: `fc2571a72f5d3c7b7b576ce2de38d91e` SHA256: `acb18a0808aedb9a5e485f1469225b9ac97f21db9af78e4cd6939700debe1cb6`
EFA 1.17.3	https://efa-installer.amazonaws.com/aws-efa-installer-1.17.3.tar.gz	MD5: `0517df4a190356ab559235147174cafd` SHA256: `5130998b0d2883bbae189b21ab215ecbc1b01ae0231659a9b4a17b0a33ebc6ca`
EFA 1.17.2	https://efa-installer.amazonaws.com/aws-efa-installer-1.17.2.tar.gz	MD5: `a329dedab53c4832df218a24449f4c9a` SHA256: `bca1fdde8b32b00346e175e597ffab32a09a08ee9ab136875fb38283cc4cd099`
EFA 1.17.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.17.1.tar.gz	MD5: `733ae2cfc9d14b52017eaf0a2ab6b0ff` SHA256: `f29322640a88ae9279805993cb836276ea240623820848463ca686c8ce02136f`

Versión	Descargar URL	Sumas de comprobación
EFA 1.17.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.17.0.tar.gz	MD5: `d430fc841563c11c3805c5f82a4746b1` SHA256: `75ab0cee4fb6bd38889dce313183f5d3a83bd233e0a6ef6205d8352821ea901d`
EFA 1.16.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.16.0.tar.gz	MD5: `399548d3b0d2e812d74dd67937b696b4` SHA256: `cecec36495a1bc6fdc82f97761a541e4fb6c9a3cbf3cfcb145acf25ea5dbd45b`
EFA 1.15.2	https://efa-installer.amazonaws.com/aws-efa-installer-1.15.2.tar.gz	MD5: `955fea580d5170b05823d51acde7ca21` SHA256: `84df4fbc1b3741b6c073176287789a601a589313accc8e6653434e8d4c20bd49`
EFA 1.15.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.15.1.tar.gz	MD5: `c4610267039f72bbe4e35d7bf53519bc` SHA256: `be871781a1b9a15fca342a9d169219260069942a8bda7a8ad06d4baeb5e2efd7`

Versión	Descargar URL	Sumas de comprobación
EFA 1.15.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.15.0.tar.gz	MD5: 9861694e1cc00d884fadac07d22898be SHA256: b329862dd5729d2d098d0507fb486bf859d7c70ce18b61c302982234a3a5c88f
EFA 1.14.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.14.1.tar.gz	MD5: 50ba56397d359e57872fde1f74d4168a SHA256: c7b1b48e86fe4b3eaa4299d3600930919c4fe6d88cc6e2c7e4a408a3f16452c7
EFA 1.14.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.14.0.tar.gz	MD5: 40805e7fd842c36ececb9fd7f921b1ae SHA256: 662d62c12de85116df33780d40e0533ef7dad92709f4f613907475a7a1b60a97
EFA 1.13.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.13.0.tar.gz	MD5: c91d16556f4fd53becadbb345828221e SHA256: ad6705eb23a3fce44af3afc0f7643091595653a723ad0374084f4f2b715192e1

Versión	Descargar URL	Sumas de comprobación
EFA 1.12.3	https://efa-installer.amazonaws.com/aws-efa-installer-1.12.3.tar.gz	MD5: 818aee81f097918cfaebd724eddea678 SHA256: 2c225321824788b8ca3fbc118207b944cdb096b847e1e0d1d853ef2f0d727172
EFA 1.12.2	https://efa-installer.amazonaws.com/aws-efa-installer-1.12.2.tar.gz	MD5: 956bb1fc5ae0d6f0f87d2e481d49fccf SHA256: 083a868a2c212a5a4fcf3e4d732b685ce39cceb3ca7e5d50d0b74e7788d06259
EFA 1.12.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.12.1.tar.gz	MD5: f5bfe52779df435188b0a2874d0633ea SHA256: 5665795c2b4f09d5f3f767506d4d4c429695b36d4a17e5758b27f033aee58900
EFA 1.12.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.12.0.tar.gz	MD5: d6c6b49fafb39b770297e1cc44fe68a6 SHA256: 28256c57e9ecc0b0778b41c1f777a9982b4e8eae782343dfe1246079933dca59

Versión	Descargar URL	Sumas de comprobación
EFA 1.11.2	https://efa-installer.amazonaws.com/aws-efa-installer-1.11.2.tar.gz	MD5: `2376cf18d1353a4551e35c33d269c404` SHA256: `a25786f98a3628f7f54f7f74ee2b39bc6734ea9374720507d37d3e8bf8ee1371`
EFA 1.11.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.11.1.tar.gz	MD5: `026b0d9a0a48780cc7406bd51997b1c0` SHA256: `6cb04baf5ffc58ddf319e956b5461289199c8dd805fe216f8f9ab8d102f6d02a`
EFA 1.11.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.11.0.tar.gz	MD5: `7d9058e010ad65bf2e14259214a36949` SHA256: `7891f6d45ae33e822189511c4ea1d14c9d54d000f6696f97be54e915ce2c9dfa`
EFA 1.10.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.10.1.tar.gz	MD5: `78521d3d668be22976f46c6fecc7b730` SHA256: `61564582de7320b21de319f532c3a677d26cc46785378eb3b95c636506b9bcb4`

Versión	Descargar URL	Sumas de comprobación
EFA 1.10.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.10.0.tar.gz	MD5: `46f73f5a7afe41b4bb918c81888fefa9` SHA256: `136612f96f2a085a7d98296da0afb6fa807b38142e2fc0c548fa986c41186282`
EFA 1.9.5	https://efa-installer.amazonaws.com/aws-efa-installer-1.9.5.tar.gz	MD5: `95edb8a209c18ba8d250409846eb6ef4` SHA256: `a4343308d7ea4dc943ccc21bcebed913e8868e59bfb2ac93599c61a7c87d7d25`
1.9.4 de EFA	https://efa-installer.amazonaws.com/aws-efa-installer-1.9.4.tar.gz	MD5: `f26dd5c350422c1a985e35947fa5aa28` SHA256: `1009b5182693490d908ef0ed2c1dd4f813cc310a5d2062ce9619c4c12b5a7f14`
1.9.3 de EFA	https://efa-installer.amazonaws.com/aws-efa-installer-1.9.3.tar.gz	MD5: `95755765a097802d3e6d5018d1a5d3d6` SHA256: `46ce732d6f3fcc9edf6a6e9f9df0ad136054328e24675567f7029edab90c68f1`

Versión	Descargar URL	Sumas de comprobación
1.8.4 de EFA	https://efa-installer.amazonaws.com/aws-efa-installer-1.8.4.tar.gz	MD5: `85d594c41e831afc6c9305263140457e` SHA256: `0d974655a09b213d7859e658965e56dc4f23a0eee2dc44bb41b6d039cc5bab45`

Topología de instancias de Amazon EC2

Al describir la topología de las instancias, se proporciona una visión jerárquica de la proximidad relativa entre estas. Puede utilizar esta información para administrar la infraestructura de computación de machine learning (ML) y computación de alto rendimiento (HPC) a escala, además de optimizar la ubicación de trabajos. Los trabajos de HPC y ML son sensibles a la latencia y al rendimiento. Puede usar la topología de las instancias para detectar su ubicación y, a continuación, usar esta información para optimizar los trabajos de HPC y ML mediante su ejecución en instancias que estén físicamente más cerca unas de otras.

Puede utilizar la topología de las instancias para detectar la ubicación de las instancias existentes, pero no puede utilizarla para elegir iniciar una nueva instancia físicamente cerca de una existente. Para influir en la ubicación de las instancias, puede utilizar Las reservas de capacidad en grupos con ubicación en clúster.

Precios

Describir la topología de las instancias no conlleva ningún costo adicional.

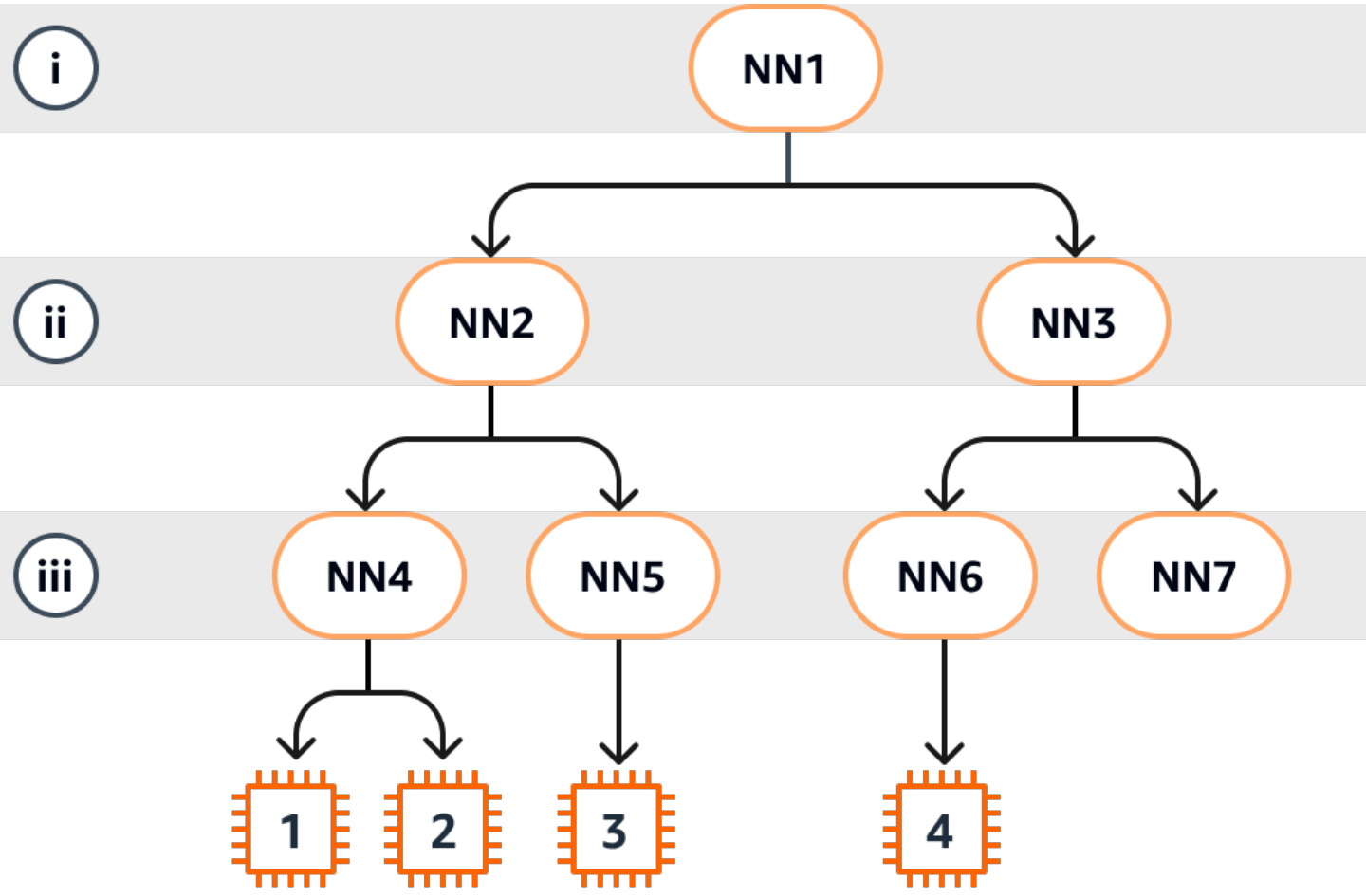
Contenido

Funcionamiento de la topología de las instancias

Cada instancia de EC2 se conecta a un conjunto de nodos. Un conjunto de nodos comprende tres nodos de red y cada nodo representa una capa diferente de la red de AWS. Las capas de red están dispuestas en una jerarquía de 3 o más capas. El conjunto de nodos proporciona una vista descendente de esta jerarquía, con la capa inferior conectada más cerca de una instancia.

La información sobre el conjunto de nodos se denomina topología de instancias.

En el siguiente diagrama, se proporciona una representación visual que se puede utilizar para comprender la topología de las instancias. Los nodos de red se identifican como NN1 – NN7. Los valores i, ii y iii identifican las capas de red. Los números 1, 2, 3 y 4 identifican las instancias de EC2. Las instancias se conectan a un nodo de la capa inferior, identificado con iii. Se puede conectar más de una instancia al mismo nodo.



En este ejemplo:

- La instancia 1 se conecta al nodo de red 4 (NN4) en la capa iii. NN4 se conecta al nodo de red 2 (NN2) en la capa ii y NN2 se conecta al nodo de red 1 (NN1) en la capa i, que es la primera de la jerarquía de la red en este ejemplo. El conjunto de nodos de red comprende NN1, NN2 y NN4, expresados jerárquicamente desde las capas superiores a la inferior.
- La instancia 2 también se conecta al nodo de red 4 (NN4). La instancia 1 y la instancia 2 comparten el mismo conjunto de nodos de red: NN1, NN2 y NN4.
- La instancia 3 también se conecta al nodo de red 5 (NN5). NN5 se conecta a NN2 y NN2 se conecta a NN1. El conjunto de nodos de red para la instancia 3 es NN1, NN2 y NN5.
- La instancia 4 se conecta al nodo de red 6 (NN6). Su conjunto de nodos de red es NN1, NN3 y NN6.

Al considerar la proximidad de las instancias 1, 2 y 3, las instancias 1 y 2 están más cerca unas de otras porque se conectan al mismo nodo de red (NN4), mientras que la instancia 3 está más alejada porque se conecta a un nodo de red diferente (NN5).

Al considerar la proximidad de todas las instancias de este diagrama, las instancias 1, 2 y 3 están más cerca unas de otras que de la instancia 4 porque comparten NN2 en su conjunto de nodos de red.

Como regla general, si el nodo de red conectado a dos instancias cualquiera es el mismo, estas instancias están físicamente cerca una de la otra, como ocurre con las instancias 1 y 2. Además, cuanto menor sea el número de saltos entre los nodos de red, más cerca estarán las instancias entre sí. Por ejemplo, las instancias 1 y 3 tienen menos saltos a un nodo de red común (NN2) que al nodo de red (NN1) que tienen en común con la instancia 4 y, por lo tanto, están más cerca unas de otras que de la instancia 4.

En este ejemplo, no hay instancias que se ejecuten en el nodo de red 7 (NN7) y, por lo tanto, la salida de la API no incluirá NN7.

Cómo interpretar la salida

La información de la topología de las instancias se obtiene mediante la API DescribeInstanceTopology. La salida proporciona una vista jerárquica de la topología de red subyacente de una instancia.

El siguiente ejemplo de salida corresponde a la información de topología de red de las cuatro instancias del diagrama anterior. A los efectos de este ejemplo, se incluyen comentarios en la salida de ejemplo.

Es importante tener en cuenta la siguiente información de la salida:

- `NetworkNodes` describe el conjunto de nodos de red de una instancia.
- En cada conjunto de nodos de red, los nodos de red se enumeran en orden jerárquico de arriba a abajo.
- El nodo de red que está conectado a la instancia es el último nodo de red de la lista (la capa inferior).
- Para determinar qué instancias están cerca unas de otras, primero busque los nodos de red comunes en la capa inferior. Si no hay nodos de red comunes en la capa inferior, busque nodos de red comunes en las capas superiores.

En la siguiente salida de ejemplo, `i-1111111111example` y `i-2222222222example` están ubicados más cerca uno del otro en comparación con las demás instancias de este ejemplo porque tienen el nodo de red `nn-4444444444example` en común en la capa inferior.

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",  //Corresponds to instance 1
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",           //Corresponds to NN1 in layer i
                "nn-2222222222example",           //Corresponds to NN2 in layer ii
                "nn-4444444444example"            //Corresponds to NN4 in layer iii -
 bottom layer, connected to the instance
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-2222222222example",  //Corresponds to instance 2
            "InstanceType": "p4d.24xlarge",
            "NetworkNodes": [
                "nn-1111111111example",           //Corresponds to NN1 - layer i
                "nn-2222222222example",           //Corresponds to NN2 - layer ii
                "nn-4444444444example"            //Corresponds to NN4 - layer iii -
 connected to instance
            ],
            "ZoneId": "usw2-az2",
```

```
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-3333333333example",  //Corresponds to instance 3
            "InstanceType": "trn1.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",           //Corresponds to NN1 - layer i
                "nn-2222222222example",           //Corresponds to NN2 - layer ii
                "nn-5555555555example"            //Corresponds to NN5 - layer iii -
 connected to instance
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-444444444example",  //Corresponds to instance 4
            "InstanceType": "trn1.2xlarge",
            "NetworkNodes": [
                "nn-1111111111example",          //Corresponds to NN1 - layer i
                "nn-3333333333example",          //Corresponds to NN3 - layer ii
                "nn-6666666666example"           //Corresponds to NN6 - layer iii -
 connected to instance
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Limitaciones

Se aplican las siguientes restricciones:

- El estado de las instancias debe ser `running`.
- Cada vista de topología de instancias es única por cuenta.
- AWS Management Console no admite la visualización de la topología de las instancias.

Requisitos previos de la topología de las instancias

Antes de describir la topología de las instancias, asegúrese de que cumplan los siguientes requisitos.

Requisitos para describir la topología de las instancias

- Regiones de AWS
- Tipos de instancias
- Estado de la instancia
- Permiso de IAM

Regiones de AWS

Regiones de AWS admitidas:

- EE. UU. Este (Norte de Virginia), EE. UU. Este (Ohio), EE. UU. Oeste (Norte de California), EE. UU. Oeste (Oregón)
- Asia Pacífico (Seúl), Asia Pacífico (Tokio)
- Canadá (centro)
- Europa (Fráncfort), Europa (Irlanda), Europa (Estocolmo)

Tipos de instancias

Tipos de instancias admitidas:

- `hpc6a.48xlarge` | `hpc6id.32xlarge` | `hpc7a.12xlarge` | `hpc7a.24xlarge` | `hpc7a.48xlarge` | `hpc7a.96xlarge` | `hpc7g.4xlarge` | `hpc7g.8xlarge` | `hpc7g.16xlarge`
- `p3dn.24xlarge` | `p4d.24xlarge` | `p4de.24xlarge` | `p5.48xlarge`
- `trn1.2xlarge` | `trn1.32xlarge` | `trn1n.32xlarge`

Consulta de los tipos de instancias disponibles en una región específica

Los tipos de instancia disponibles varían según la región. Para comprobar si un tipo de instancia está disponible en una región, use el comando describe-instance-types-offerings con el parámetro `--region`. Incluya el parámetro `--filters` para limitar los resultados al tipo o familia de instancias que le interese y el parámetro `--query` para limitar la salida al valor de `InstanceType`.

```
aws ec2 describe-instance-type-offerings \
    --region us-east-2 \
    --filters 'Name=instance-type, Values=trn1*' \
```

```
    --query 'InstanceTypeOfferings[].InstanceType'
```

Resultado previsto

```
[
    "trn1.2xlarge",
    "trn1.32xlarge",
    "trn1n.32xlarge"
]
```

Estado de la instancia

Las instancias deben tener el estado `running`. No puede obtener información sobre la topología de las instancias que se encuentran en otro estado.

Permiso de IAM

La identidad de IAM (usuario, grupo de usuarios o rol) requiere el siguiente permiso de IAM:

- `ec2:DescribeInstanceTopology`

Ejemplos de la topología de las instancias de Amazon EC2

Puede usar el comando describe-instance-topology de la CLI para describir la topología de las instancias de EC2.

Si utiliza el comando `describe-instance-topology` sin parámetros ni filtros, en la respuesta se incluyen todas las instancias que coincidan con los tipos de instancias compatibles con este comando en la región especificada. Para especificar la región, incluya el parámetro `--region` o establezca una región predeterminada. Para obtener más información sobre cómo establecer una región predeterminada, consulte Especificar la región para un recurso.

Puede incluir parámetros para devolver instancias que coincidan con los ID de instancia o los nombres de los grupos de ubicación especificados. También puede incluir filtros para devolver instancias que coincidan con un tipo o familia de instancias específico, o instancias en una zona de disponibilidad o zona local específica. Puede incluir un único parámetro o filtro, o una combinación de parámetros y filtros.

La salida está paginada, con hasta 20 instancias por página de forma predeterminada. Puede especificar hasta 100 instancias por página mediante el parámetro `--max-results`.

Para obtener más información, consulte describe-instance-topology en la Referencia de los comandos de AWS CLI.

Permisos necesarios

Se requiere el siguiente permiso para describir la topología de las instancias:

- `ec2:DescribeInstanceTopology`

Ejemplos

Ejemplo 1: sin parámetros ni filtros

Descripción de la topología de todas sus instancias

Utilice el comando describe-instance-topology de la CLI sin especificar ningún parámetro o filtro.

```
aws ec2 describe-instance-topology --region us-west-2
```

En la respuesta se devuelven solo las instancias que coinciden con los tipos de instancias compatibles con esta API. Las instancias pueden estar en diferentes zonas de disponibilidad, zonas locales (`ZoneId`) y grupos de ubicación (`GroupName`). Si una instancia no está en un grupo de

ubicación, el campo `GroupName` no aparecerá en la salida. En la siguiente salida de ejemplo, solo una instancia está en un grupo de ubicación.

Ejemplo de resultado


```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "my-ml-cpg",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "p4d.24xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-3333333333example",
            "InstanceType": "trn1.32xlarge",
            "NetworkNodes": [
                "nn-1212121212example",
                "nn-1211122211example",
                "nn-1311133311example"
            ],
            "ZoneId": "usw2-az4",
            "AvailabilityZone": "us-west-2d"
        },
        {
            "InstanceId": "i-444444444example",
            "InstanceType": "trn1.2xlarge",
```

```
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-5434334334example",
                "nn-1235301234example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Ejemplo 2: filtro de tipo de instancia

Puede filtrar por un tipo de instancia específico (coincidencia exacta) o por una familia de instancias (con un comodín). También puede combinar un filtro de tipo de instancia y un filtro de familia de instancias específicos.

Ejemplo 2a: filtro de coincidencia exacta para un tipo de instancia específico

Descripción de la topología de todas las instancias que coinciden con un tipo de instancia específico

Utilice el comando describe-instance-topology de la CLI con el filtro `instance-type`. En este ejemplo, la salida se filtra para las instancias `trn1n.32xlarge`. En la respuesta se devolverán solo las instancias que coincidan con el tipo de instancia especificado.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --filters Name=instance-type,Values=trn1n.32xlarge
```

Ejemplo de resultado

```
{
    "Instances": [
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
```

```
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Ejemplo 2b: filtro comodín para una familia de instancias

Descripción de la topología de todas las instancias que coinciden con una familia de instancias específica

Utilice el comando describe-instance-topology de la CLI con el filtro `instance-type`. En este ejemplo, la salida se filtra para las instancias `trn1*`. En la respuesta se devolverán solo las instancias que coincidan con la familia de instancias especificada.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --filters Name=instance-type,Values=trn1*
```

Ejemplo de resultado

```
{
    "Instances": [
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-3333333333example",
            "InstanceType": "trn1.32xlarge",
            "NetworkNodes": [
                "nn-1212121212example",
                "nn-1211122211example",
```

```
                "nn-1311133311example"
            ],
            "ZoneId": "usw2-az4",
            "AvailabilityZone": "us-west-2d"
        },
        {
            "InstanceId": "i-444444444example",
            "InstanceType": "trn1.2xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-5434334334example",
                "nn-1235301234example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Ejemplo 2c: filtros combinados de familia de instancias y coincidencia exacta

Descripción de la topología de todas las instancias que coinciden con una familia o tipo de instancias específico

Utilice el comando describe-instance-topology de la CLI con el filtro `instance-type`. En este ejemplo, la salida se filtra para las instancias `pd4d*` o `trn1n.32xlarge`. En la respuesta se devolverán las instancias que coincidan con alguno de los filtros especificados.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --filters "Name=instance-type,Values=p4d*,trn1n.32xlarge"
```

Ejemplo de resultado

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
```

```
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-4343434343example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Ejemplo 3: filtro de ID de zona

Puede usar el filtro `zone-id` para filtrar por zona de disponibilidad o zona local. También puede combinar un filtro de zona de disponibilidad y un filtro de zona local.

Ejemplo 3a: filtro de zona de disponibilidad

Descripción de la topología de todas las instancias que coinciden con una zona de disponibilidad específica

Utilice el comando describe-instance-topology de la CLI con el filtro `zone-id`. En este ejemplo, la salida se filtra con el ID de la zona de disponibilidad `use1-az1`. En la respuesta se devolverán solo las instancias que coincidan con la zona de disponibilidad especificada.

```
aws ec2 describe-instance-topology \
    --region us-east-1 \
    --filters Name=zone-id,Values=use1-az1
```

Ejemplo de resultado

```
{
    "Instances": [
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "ZoneId": "use1-az1",
            "AvailabilityZone": "us-east-1a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Ejemplo 3b: filtro de zona local

Descripción de la topología de todas las instancias que coinciden con una zona local específica

Utilice el comando describe-instance-topology de la CLI con el filtro `zone-id`. En este ejemplo, la salida se filtra con el ID de la zona local `use1-atl2-az1`. En la respuesta se devolverán solo las instancias que coincidan con la zona local especificada.

```
aws ec2 describe-instance-topology \
    --region us-east-1 \
    --filters Name=zone-id,Values=use1-atl2-az1
```

Ejemplo de resultado

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
```

```
            ],
            "ZoneId": "use1-atl2-az1",
            "AvailabilityZone": "us-east-1-atl-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Ejemplo 3c: filtros combinados de zona de disponibilidad y zona local

Descripción de la topología de todas las instancias que coinciden con una zona de disponibilidad o zona local específica

Utilice el comando describe-instance-topology de la CLI con el filtro `zone-id`. En este ejemplo, la salida se filtra con el ID de la zona de disponibilidad `use1-az1` y el de la zona local `use1-atl2-az1`. En la respuesta se devolverán las instancias que coincidan con alguno de los filtros especificados.

```
aws ec2 describe-instance-topology \
    --region us-east-1 \
    --filters Name=zone-id,Values=use1-az1,use1-atl2-az1
```

Ejemplo de resultado

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "use1-atl2-az1",
            "AvailabilityZone": "us-east-1-atl-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
```

```
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "ZoneId": "use1-az1",
            "AvailabilityZone": "us-east-1a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Ejemplo 4: filtros combinados de tipo de instancia e ID de zona

Puede combinar todos los filtros en un único comando.

Descripción de la topología de todas las instancias que coinciden con un tipo de instancia, familia de instancias, zona de disponibilidad o zona local específicos

Utilice el comando describe-instance-topology de la CLI con los filtros `instance-type` y `zone-id`. En este ejemplo, la salida se filtra para la familia de instancias `p4d*`, el tipo de instancia `trn1n.32xlarge`, el ID de la zona de disponibilidad `use1-az1` y el ID la zona local `use1-atl2-az1`. En la respuesta se devolverán las instancias que coincidan con las instancias `p4d*` o `trn1n.32xlarge` de las zonas `us-east-1a` o `us-east-1-atl-2a`.

```
aws ec2 describe-instance-topology \
    --region us-east-1 \
    --filters "Name=instance-type,Values=p4d*,trn1n.32xlarge" "Name=zone-
id,Values=use1-az1,use1-atl2-az1"
```

Ejemplo de resultado

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
```

```
            ],
            "ZoneId": "use1-atl2-az1",
            "AvailabilityZone": "us-east-1-atl-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "ZoneId": "use1-az1",
            "AvailabilityZone": "us-east-1a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Ejemplo 5: parámetro de nombre de grupo de ubicación

Descripción de la topología de todas las instancias de un grupo de ubicación específico

Use el comando describe-instance-topology de la CLI con el parámetro `group-names`. En el siguiente ejemplo, las instancias pueden estar en el grupo de ubicación `ML-group` o `HPC-group`. En la respuesta se devolverán las instancias que estén en cualquiera de los grupos de ubicación.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --group-names ML-group HPC-group
```

Ejemplo de resultado

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
```

```
                "nn-3333333333example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "GroupName": "HPC-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Ejemplo 6: ID de instancia

Descripción de la topología de instancias especificadas

Use el comando describe-instance-topology de la CLI con el parámetro `--instance-ids`. En la respuesta se devolverán las instancias que coincidan con los ID de instancia especificados.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --instance-ids i-1111111111example i-2222222222example
```

Ejemplo de resultado

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
```

```
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "GroupName": "HPC-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Grupos de ubicación

Para satisfacer las necesidades de su carga de trabajo, puede iniciar un grupo de instancias de EC2 interdependientes en un grupo de ubicación para influir en su ubicación.

Dependiendo del tipo de carga de trabajo, puede crear un grupo de ubicación con una de las siguientes estrategias de ubicación:

- Clúster: agrupa las instancias unas cerca de otras dentro de una zona de disponibilidad. Esta estrategia le permite que las cargas de trabajo alcancen el rendimiento de red de baja latencia necesario para una comunicación entre nodos estrechamente acoplada, típica de las aplicaciones de computación de alto rendimiento (HPC).
- Partición: distribuye las instancias entre las particiones lógicas de modo que los grupos de instancias de una partición no compartan el hardware subyacente con los grupos de instancias de las demás particiones. Esta estrategia suelen utilizarla grandes cargas de trabajo distribuidas y replicadas, como Hadoop, Cassandra y Kafka.
- Reparto: coloca estrictamente un pequeño grupo de instancias en distintos equipos de hardware subyacentes para reducir los fallos correlacionados.

Los grupos de ubicación son opcionales. Si no inicia las instancias en un grupo de ubicación, EC2 intenta colocar las instancias de forma que todas las instancias se distribuyan en el hardware subyacente para minimizar los errores correlacionados.

La creación de un grupo de ubicación no supone ningún cargo adicional.

Estrategias de ubicación

Puede crear un grupo con ubicación mediante una de las siguientes estrategias de ubicación.

Estrategias de ubicación:

- Grupos de ubicación en clúster
- Grupos de ubicación de particiones
- Grupos de ubicación distribuida

Grupos de ubicación en clúster

Un grupo de ubicación en clúster es una agrupación lógica de instancias en una misma zona de disponibilidad. Un grupo con ubicación en clúster puede abarcar redes privadas virtuales (VPC) interconectadas en la misma región. Las instancias del mismo grupo de ubicación en clúster disfrutan de un límite de rendimiento por flujo más alto para el tráfico TCP/IP y se colocan en el mismo segmento de ancho de banda con una alta capacidad de biseccionado de la red.

La imagen siguiente muestra las instancias colocadas en un grupo con ubicación en clúster.

Los grupos con ubicación en clúster están recomendados para aplicaciones que se benefician de una baja latencia de red, un elevado rendimiento de la red o ambas cosas. También son recomendables cuando la mayor parte del tráfico de red se da entre las instancias del grupo. Para

proporcionar la latencia más baja y el mayor rendimiento de red de paquetes por segundo para el grupo de ubicación, elija un tipo de instancia que admita redes mejoradas. Para obtener más información, consulte Redes mejoradas.

Le recomendamos que lance las instancias de la siguiente forma:

- Utilice una única solicitud de inicialización para iniciar el número de instancias que necesite en el grupo de ubicación.
- Utilice el mismo tipo de instancia con todas las instancias del grupo de ubicación.

Si intenta añadir más instancias al grupo de ubicación más adelante, o si intenta iniciar más de un tipo de instancia en el grupo de ubicación, aumenta las posibilidades de obtener un error de capacidad insuficiente.

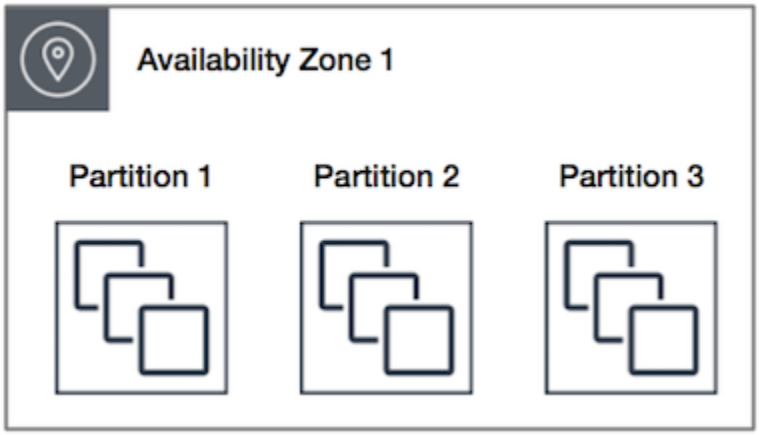
Si detiene una instancia en un grupo de ubicación y, a continuación, la vuelve a iniciar, se seguirá ejecutando en el grupo de ubicación. No obstante, si no hay suficiente capacidad para la instancia, se generará un error al iniciarla.

Si recibe un error de capacidad al iniciar una instancia en un grupo de ubicación que ya tiene instancias en ejecución, detenga e inicie todas las instancias en el grupo de ubicación y vuelva a intentar la inicialización. Al iniciar las instancias, estas podrían migrar a un hardware que tuviera capacidad para todas las instancias solicitadas.

Grupos de ubicación de particiones

Los grupos de ubicación de partición ayudan a reducir la probabilidad de errores de hardware correlacionados para su aplicación. Cuando se utilizan los grupos de ubicación de particiones, Amazon EC2 divide cada grupo en segmentos lógicos denominados particiones. Amazon EC2 se asegura de que cada partición dentro de un grupo de ubicación tenga su propio juego de bastidores. Cada bastidor tiene su propia red y fuente de alimentación. No hay dos particiones dentro de un grupo de ubicación que compartan los mismos bastidores, lo que le permite aislar el impacto de los errores de hardware en la aplicación.

La imagen siguiente es una representación visual sencilla de un grupo de ubicación de partición en una única zona de disponibilidad. Muestra instancias que se colocan en un grupo de ubicación de partición con tres particiones: Partición 1, Partición 2 y Partición 3. Cada partición contiene varias instancias. Las instancias de una partición no comparten bastidores con las instancias de las demás particiones, lo que permite contener el impacto de un único error de hardware en una sola partición asociada.



Los grupos de ubicación de particiones se pueden utilizar para implementar cargas de trabajo de gran tamaño distribuidas y replicadas como HDFS, HBase y Cassandra entre distintos bastidores. Al iniciar instancias en un grupo con ubicación en particiones, Amazon EC2 intenta distribuir las instancias de manera uniforme entre el número de particiones que especifique. También puede iniciar las instancias en una partición determinada, para tener más control sobre dónde se ubican las instancias.

Un grupo de ubicación de particiones puede tener particiones en varias zonas de disponibilidad en la misma región. Un grupo de ubicación de particiones puede tener un máximo de siete particiones por zona de disponibilidad. El número de instancias que se pueden iniciar en un grupo con ubicación en particiones viene limitado solamente por los límites de la cuenta.

Además, los grupos con ubicación en particiones ofrecen visibilidad sobre las particiones — es decir, puede ver qué instancias hay en cada partición. Puede compartir esta información con aplicaciones que tienen en cuenta la topología, tales como HDFS, HBase y Cassandra. Estas aplicaciones utilizan esta información para tomar decisiones inteligentes de replicación de datos con el fin de aumentar la disponibilidad y durabilidad de los datos.

Si inicia o inicia una instancia en un grupo con ubicación en particiones y no hay suficiente hardware exclusivo para atender la solicitud, dicha solicitud produce un error. Amazon EC2 pone a disposición más hardware distinto posteriormente, de modo que pueda volver a enviar la solicitud más tarde.

Grupos de ubicación distribuida

Un grupo con ubicación distribuida es un grupo de instancias que se colocan en un equipo distinto.

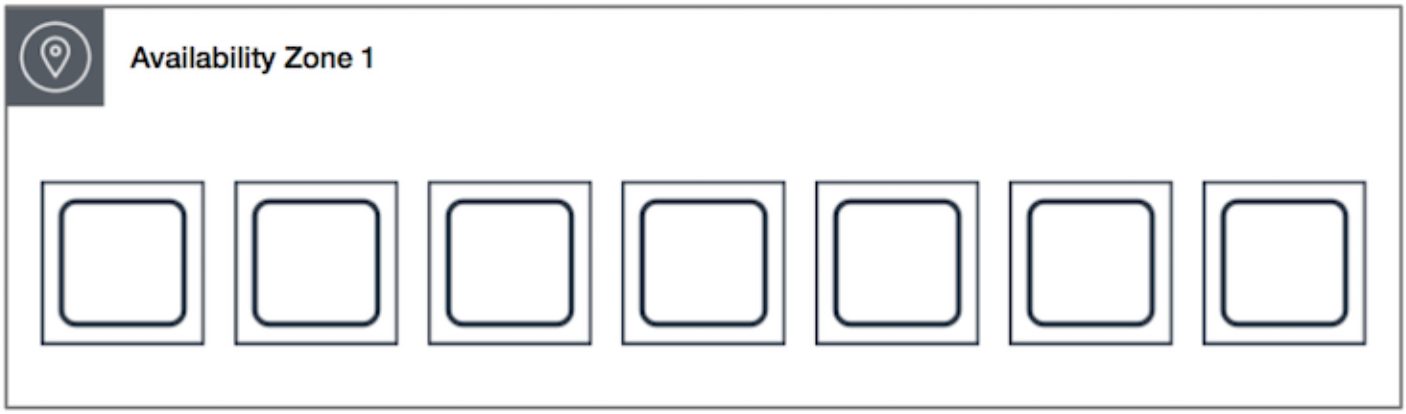
Se recomienda usar grupos con ubicación distribuida en aplicaciones con pocas instancias críticas que deben mantenerse separadas entre sí. iniciar instancias en un grupo de ubicación a nivel

de distribución reduce el riesgo de errores simultáneos que puedan ocurrir cuando las instancias comparten el mismo equipo. Los grupos de ubicación a nivel de distribución proporcionan acceso a distinto equipo, por lo que son adecuados para mezclar tipos de instancias o para iniciar instancias con el tiempo.

Si inicia o inicia una instancia en un grupo con ubicación distribuida y no hay suficiente hardware exclusivo para atender la solicitud, dicha solicitud produce un error. Amazon EC2 pone a disposición más hardware distinto posteriormente, de modo que pueda volver a enviar la solicitud más tarde. Los grupos de ubicación pueden distribuir instancias entre bastidores o hosts. Los grupos con ubicación distribuida de bastidor se pueden usar en las regiones de AWS y en AWS Outposts. Solo puede usar grupos con ubicación distribuida de host con AWS Outposts.

Grupo con ubicación distribuida de host

La imagen siguiente muestra siete instancias en una sola zona de disponibilidad colocadas en un grupo con ubicación distribuida. Las siete instancias se colocan en siete bastidores distintos. Cada bastidor tiene su propia red y fuente de alimentación.



Un grupo con ubicación distribuida de bastidor puede abarcar varias zonas de disponibilidad en la misma región. En una región, un grupo con ubicación distribuida de bastidor puede tener hasta siete instancias en ejecución por zona de disponibilidad por grupo. Con Outposts, un grupo con ubicación distribuida de bastidor puede contener tantas instancias como bastidores tenga en su implementación de Outpost.

Grupos con ubicación distribuida a nivel de host

Los grupos con ubicación distribuida de host solo están disponibles con AWS Outposts. Un grupo con ubicación distribuida de host puede contener tantas instancias como hosts tenga en su

implementación de Outpost. Para obtener más información, consulte the section called “Grupos de ubicación en AWS Outposts”.

Reglas y limitaciones de los grupos de ubicación

Temas

Reglas y limitaciones generales

Antes de utilizar grupos de ubicación, tenga en cuenta las siguientes reglas:

- Puede crear un máximo de 500 grupos de ubicación por cuenta en cada región.
- El nombre que especifique para el grupo de ubicación debe ser el único de esa región en la cuenta de AWS.
- No se pueden fusionar grupos de ubicación.
- Una instancia se puede iniciar en un grupo de ubicación a la vez; no puede abarcar varios grupos de ubicación.
- Las reservas de capacidad bajo demanda y las instancias reservadas de zona permiten reservar capacidad para instancias de EC2 en zonas de disponibilidad. Al iniciar una instancia, si los atributos de la instancia coinciden con los especificados en una reserva de capacidad bajo demanda o una instancia reservada de zona, la instancia utiliza automáticamente la capacidad reservada. Esto también se aplica si inicia la instancia en un grupo con ubicación.

  Si tiene pensado iniciar instancias en un grupo con ubicación en clúster, le recomendamos que reserve la capacidad de forma explícita en el grupo con ubicación en clúster. Para ello, puede crear una reserva de capacidad bajo demanda en un grupo con ubicación en clúster especificado. Tenga en cuenta que, si bien puede reservar capacidad de esta manera mediante las reservas de capacidad bajo demanda, no se puede hacer lo mismo con las instancias reservadas de zona, ya que no pueden reservar capacidad de forma explícita en un grupo con ubicación.
- No se puede iniciar host dedicados en grupos de ubicación.
- No se puede iniciar una instancia de spot que esté configurada para detenerse o hibernar en caso de interrupción en un grupo de ubicación.

Reglas y limitaciones de los grupos de ubicación en clúster

Los grupos de ubicación en clúster están sujetos a las siguientes reglas:

- Se admiten los siguientes tipos de instancias:
  - Instancias de la generación actual, excepto instancias de rendimiento ampliable (por ejemplo, T2), instancias Mac1 e instancias M7i-flex.
  - Las siguientes instancias de la generación anterior: A1, C3, C4, I2, M4, R3 y R4.
- Un grupo de ubicación en clúster no puede abarcar varias zonas de disponibilidad.
- La máxima velocidad de tráfico de rendimiento de red entre dos instancias en un grupo de ubicación en clúster está limitada por la más lenta de las dos instancias. Para aplicaciones que requieran un rendimiento elevado, elija un tipo de instancia con conexión de red que cumpla con sus requisitos.
- Las instancias que están habilitadas para las redes mejoradas están sujetas a las reglas siguientes:
  - Las instancias dentro de un grupo de ubicación en clúster pueden usar hasta 10 Gbps para tráfico de un solo flujo. Las instancias que no están dentro de un grupo de ubicación en clúster pueden usar hasta 5 Gbps para tráfico de un solo flujo.
  - El tráfico desde y hacia buckets de Amazon S3 dentro de la misma región en un espacio de direcciones IP públicas o a través de un punto de conexión de VPC puede utilizar todo el ancho de banda de instancias disponible en conjunto.
- Puede iniciar varios tipos de instancias en un grupo de ubicación en clúster. Sin embargo, esto reduce la probabilidad de que se disponga de la capacidad necesaria para que la inicialización se realice correctamente. Le recomendamos usar el mismo tipo de instancia para todas las instancias de un mismo grupo con ubicación en clúster.
- El tráfico de red a Internet y a través de una conexión de AWS Direct Connect hacia los recursos en las instalaciones está limitado a 5 Gbps en el caso de los grupos con ubicación en clúster.

Reglas y limitaciones de los grupos con ubicación en particiones

Los grupos con ubicación en particiones están sujetos a las siguientes reglas:

- Un grupo con ubicación en particiones admite un máximo de siete particiones por zona de disponibilidad. El número de instancias que se pueden iniciar en un grupo con ubicación en particiones viene limitado solamente por los límites de la cuenta.

- Cuando las instancias se inician en un grupo con ubicación en particiones, Amazon EC2 intenta distribuir las instancias de manera uniforme entre todas las particiones. Amazon EC2 no garantiza que lo consiga.
- Un grupo con ubicación en particiones con instancias dedicadas puede tener un máximo de dos particiones.
- Las reservas de capacidad no cumplen su función en un grupo con ubicación en partición.

Reglas y limitaciones de los grupos de ubicación distribuida

Los grupos de ubicación distribuida están sujetos a las siguientes reglas:

- Un grupo con ubicación distribuida de bastidor admite hasta siete instancias en ejecución por zona de disponibilidad. Por ejemplo, en una región con tres zonas de disponibilidad, se pueden ejecutar hasta 21 instancias en el grupo, con siete instancias por cada zona de disponibilidad. Si intenta comenzar una octava instancia en la misma zona de disponibilidad y en el mismo grupo con ubicación distribuida, la instancia no se iniciará. Si necesita más de siete instancias en una zona de disponibilidad, le recomendamos que use varios grupos con ubicación distribuida. El uso de varios grupos con ubicación distribuida no garantiza la distribución de instancias entre grupos, pero sí la asegura en cada grupo, lo cual limita el impacto de ciertas clases de errores.
- Las instancias dedicadas no admiten grupos con ubicación distribuida.
- Los grupos con ubicación distribuida a nivel de host solo se admiten para grupos de ubicación en AWS Outposts. Un grupo con ubicación distribuida de host puede contener tantas instancias como hosts tenga en su implementación de Outpost.
- En una región, un grupo con ubicación distribuida de bastidor puede tener hasta siete instancias en ejecución por zona de disponibilidad por grupo. Con AWS Outposts, un grupo con ubicación distribuida de bastidor puede contener tantas instancias como bastidores tenga en su implementación de Outpost.
- Las reservas de capacidad no cumplen su función en un grupo con ubicación distribuida.

Trabajo con grupos con ubicación

Contenido

- Iniciar instancias en un grupo de ubicación
- Describir instancias en un grupo de ubicación
- Cambiar el grupo de ubicación para una instancia
- Puede quitar una instancia de un grupo de ubicación
- Eliminar un grupo de ubicación

Crear un grupo de ubicación

Puede crear un grupo de ubicación utilizando uno de los siguientes comandos:

Console

Para crear un grupo de ubicación mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Grupos de ubicación.
3. Elija Crear grupo con ubicación.
4. Especifique un nombre para el grupo.
5. Elija la estrategia de ubicación del grupo.
   - Si elige Distribuir, elige el nivel de distribución.
     - Bastidor: sin restricciones
     - Host: solo para Outposts
   - Si elige Partición, especifique el número de particiones que habrá dentro del grupo.
6. Para etiquetar el grupo de ubicación, elija Agregar etiqueta y luego, ingrese una clave y un valor. Para cada etiqueta que desee agregar, elija Agregar etiqueta.
7. Elija Crear grupo.

AWS CLI

Para crear un grupo de ubicación con la AWS CLI

Utilice el comando create-placement-group. En el ejemplo siguiente se crea un grupo de ubicación denominado `my-cluster` que utiliza la estrategia de ubicación `cluster` y se aplica una etiqueta con una clave de `purpose` y un valor de `production`.

```
aws ec2 create-placement-group \
    --group-name my-cluster \
    --strategy cluster \
    --tag-specifications 'ResourceType=placement-
group,Tags={Key=purpose,Value=production}'
```

Para crear un grupo de ubicación de particiones con la AWS CLI

Utilice el comando create-placement-group. Especifique el parámetro `--strategy` con el valor `partition` y el parámetro `--partition-count` con el número de particiones que desee. En este ejemplo, el grupo de ubicación de particiones se llama `HDFS-Group-A` y se crea con cinco particiones.

```
aws ec2 create-placement-group \
    --group-name HDFS-Group-A \
    --strategy partition \
    --partition-count 5
```

PowerShell

Para crear un grupo de ubicación con la AWS Tools for Windows PowerShell

Utilice el comando New-EC2PlacementGroup.

Visualización de información de los grupos con ubicación

Puede ver todos los grupos con ubicación e información sobre ellos mediante uno de los métodos siguientes.

Console

Para ver información sobre uno o varios grupos con ubicación

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Red y seguridad, seleccione Grupos de ubicación.
3. En la tabla Grupos de ubicación, puede ver la siguiente información para cada grupo con ubicación:

   - Nombre del grupo: nombre que asignó al grupo con ubicación.

- ID del grupo: ID del grupo con ubicación.
- Estrategia: estrategia de ubicación del grupo con ubicación.
- Estado: estado del grupo con ubicación.
- Partición: número de particiones. Solo es válido solo si la estrategia es partición.
- ARN del grupo: nombre de recurso de Amazon (ARN) del grupo con ubicación.

AWS CLI

Para describir todos los grupos con ubicación

Utilice el comando describe-placement-groups de la AWS CLI.

```
aws ec2 describe-placement-groups
```

Ejemplo de respuesta

```
{
    "PlacementGroups": [
        {
            "GroupName": "my-cluster-pg",
            "State": "available",
            "Strategy": "cluster",
            "GroupId": "pg-0123456789example",
            "GroupArn": "arn:aws:ec2:eu-west-1:111111111111:placement-group/my-
cluster-pg"
        },
            ...
     ]
}
```

Para describir un grupo con ubicación especificado

Utilice el comando describe-placement-groups de la AWS CLI. Puede especificar el parámetro `--group-id` o `--group-name`.

Especifique el ID del grupo con ubicación:

```
aws ec2 describe-placement-groups --group-id pg-0123456789example
```

Especifique el nombre del grupo con ubicación:

```
aws ec2 describe-placement-groups --group-name my-cluster-pg
```

Ejemplo de respuesta

```
{
    "PlacementGroups": [
        {
            "GroupName": "my-cluster-pg",
            "State": "available",
            "Strategy": "cluster",
            "GroupId": "pg-0123456789example",
            "GroupArn": "arn:aws:ec2:eu-west-1:111111111111:placement-group/my-
cluster-pg"
        }
    ]
}
```

Etiquetar un grupo de ubicación

Para ayudar a clasificar y administrar los grupos de ubicación existentes, puede etiquetarlos con metadatos personalizados. Para obtener más información sobre cómo funcionan las etiquetas, consulte Etiquetar los recursos de Amazon EC2.

Al etiquetar un grupo de ubicación, las instancias que se inician en el grupo de ubicación no se etiquetan automáticamente. Debe etiquetar explícitamente las instancias que se lancen en el grupo de ubicación. Para obtener más información, consulte Agregar una etiqueta cuando lanza una instancia.

Puede ver, agregar y eliminar etiquetas mediante uno de los siguientes métodos.

Console

Para ver, agregar o eliminar una etiqueta de un grupo de ubicación existente

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Grupos de ubicación.
3. Seleccione el grupo de ubicación y, a continuación, elija Acciones, Administrar etiquetas.
4. La pantalla Administrar etiquetas muestra las etiquetas asignadas al grupo con ubicación.

- Para agregar una etiqueta, elija Agregar etiqueta y, a continuación, escriba la clave y el valor de la etiqueta. Puede agregar hasta 50 etiquetas por grupo de ubicación. Para obtener más información, consulte Restricciones de las etiquetas.
- Para eliminar una etiqueta, elija Eliminar junto a la etiqueta que desee eliminar.

5. Seleccione Guardar.

AWS CLI

Para ver las etiquetas de grupo de ubicación

Utilice el comando describe-tags para ver las etiquetas del recurso especificado. En el siguiente ejemplo, se describen las etiquetas de todos los grupos de ubicación.

```
aws ec2 describe-tags \
    --filters Name=resource-type,Values=placement-group
```

```
{
    "Tags": [
        {
            "Key": "Environment",
            "ResourceId": "pg-0123456789EXAMPLE",
            "ResourceType": "placement-group",
            "Value": "Production"
        },
        {
            "Key": "Environment",
            "ResourceId": "pg-9876543210EXAMPLE",
            "ResourceType": "placement-group",
            "Value": "Production"
        }
    ]
}
```

También puede utilizar el comando describe-tags para ver las etiquetas de un grupo de ubicación. Para hacerlo, deberá especificar su ID. En el siguiente ejemplo, se describen las etiquetas de pg-0123456789EXAMPLE.

```
aws ec2 describe-tags \
```

```
    --filters Name=resource-id,Values=pg-0123456789EXAMPLE
```

```
{
    "Tags": [
        {
            "Key": "Environment",
            "ResourceId": "pg-0123456789EXAMPLE",
            "ResourceType": "placement-group",
            "Value": "Production"
        }
    ]
}
```

Para ver las etiquetas de un grupo de ubicación debe describir el grupo de ubicación.

Utilice el comando describe-placement-groups para ver la configuración del grupo de ubicación especificado, que incluye las etiquetas especificadas para el grupo de ubicación.

```
aws ec2 describe-placement-groups \
    --group-name my-cluster
```

```
{
    "PlacementGroups": [
        {
            "GroupName": "my-cluster",
            "State": "available",
            "Strategy": "cluster",
            "GroupId": "pg-0123456789EXAMPLE",
            "Tags": [
                {
                    "Key": "Environment",
                    "Value": "Production"
                }
            ]
        }
    ]
}
```

Para etiquetar un grupo de ubicación existente mediante la AWS CLI

Puede utilizar el comando create-tags para etiquetar recursos existentes. En el siguiente ejemplo, el grupo con ubicación existente se etiqueta con `Key=Cost-Center` y `Value=CC-123`.

```
aws ec2 create-tags \
    --resources pg-0123456789EXAMPLE \
    --tags Key=Cost-Center,Value=CC-123
```

Para eliminar una etiqueta de un grupo de ubicación con la AWS CLI

Puede utilizar el comando delete-tags para eliminar etiquetas de los recursos existentes. Para obtener ejemplos, consulte Examples (Ejemplos) en la Referencia de comandos de la AWS CLI.

PowerShell

Para ver las etiquetas de grupo de ubicación

Utilice el comando Get-EC2Tag.

Para describir las etiquetas de un grupo de ubicación específico

Utilice el comando Get-EC2PlacementGroup.

Para etiquetar un grupo de ubicación existente

Utilice el comando New-EC2Tag.

Para eliminar una etiqueta de un grupo de ubicación

Utilice el comando Remove-EC2Tag.

Iniciar instancias en un grupo de ubicación

Puede iniciar una instancia en un grupo de ubicación si se cumplen las reglas y limitaciones del grupo de ubicación utilizando uno de los métodos siguientes.

Console

Iniciar instancias en un grupo con ubicación

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de la consola de EC2, en la sección Iniciar instancia, elija Iniciar instancia. Complete el formulario tal como se le indica, procurando realizar lo siguiente:
   - En Tipo de instancia, seleccione un tipo de instancia que se pueda iniciar en un grupo de ubicación.

- En el cuadro Resumen, bajo Número de instancias, ingrese el número total de instancias que necesita en este grupo de ubicación, ya que es posible que no pueda agregar más instancias más adelante.
- En Detalles avanzados, en Nombre del grupo de ubicación, puede elegir agregar las instancias a un grupo de ubicación nuevo o existente. Si elige un grupo de ubicación con una estrategia de partición, en Partición de destino, elija la partición en la que desea iniciar las instancias.

AWS CLI

Lanzar instancias en un grupo con ubicación

Utilice el comando run-instances y especifique el nombre del grupo de ubicación con el parámetro `--placement "GroupName = my-cluster"`. En este ejemplo, el grupo de ubicación se llama `my-cluster`.

```
aws ec2 run-instances --placement "GroupName = my-cluster"
```

Para iniciar instancias en una partición específica de un grupo de ubicación de particiones con la AWS CLI

Utilice el comando run-instances y especifique el nombre del grupo de ubicación y la partición con el parámetro `--placement "GroupName = HDFS-Group-A, PartitionNumber = 3"`. En este ejemplo, el grupo de ubicación de particiones se llama `HDFS-Group-A` y el número de partición es `3`.

```
aws ec2 run-instances --placement "GroupName = HDFS-Group-A, PartitionNumber = 3"
```

PowerShell

Para iniciar instancias en un grupo de ubicación con AWS Tools for Windows PowerShell

Utilice el comando New-EC2Instance y especifique el nombre del grupo de ubicación con el parámetro `-Placement_GroupName`.

Describir instancias en un grupo de ubicación

Puede ver la información de ubicación de las instancias utilizando uno de los métodos siguientes. También puede filtrar los grupos de ubicación de particiones por el número de partición a través de la AWS CLI.

Console

Ver el grupo con ubicación y el número de partición de una instancia

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instancias.
3. Seleccione la instancia.
4. En la pestaña Detalles, en Host y grupo de ubicación, busque Grupo de ubicación. Si la instancia no está en un grupo de ubicación, el campo está vacío. De lo contrario, contiene el nombre del grupo de ubicación. Si el grupo de ubicación es un grupo con ubicación en particiones, Número de partición contiene el número de partición de la instancia.

AWS CLI

Ver el número de partición de una instancia en un grupo con ubicación en particiones

Utilice el comando describe-instances y especifique el parámetro `--instance-id`.

```
aws ec2 describe-instances --instance-id i-0123a456700123456
```

La respuesta contiene la información de ubicación, que incluye el nombre del grupo de ubicación y el número de partición de la instancia.

```
"Placement": {
     "AvailabilityZone": "us-east-1c",
     "GroupName": "HDFS-Group-A",
     "PartitionNumber": 3,
     "Tenancy": "default"
}
```

Filtrar las instancias para un grupo con ubicación en particiones y un número de partición específicos

Utilice el comando describe-instances y especifique el parámetro `--filters` con los filtros `placement-group-name` y `placement-partition-number`. En este ejemplo, el grupo de ubicación de particiones se llama `HDFS-Group-A` y el número de partición es 7.

```
aws ec2 describe-instances --filters "Name = placement-group-name, Values = HDFS-Group-A" "Name = placement-partition-number, Values = 7"
```

La respuesta enumera todas las instancias que se encuentran en la partición especificada dentro del grupo de ubicación determinado. A continuación, se incluye un ejemplo del resultado que muestra solo el ID de instancia, el tipo de instancia y la información de ubicación para las instancias devueltas.

```
"Instances": [
                {
                    "InstanceId": "i-0a1bc23d4567e8f90",
                    "InstanceType": "r4.large",
                    },

                    "Placement": {
                        "AvailabilityZone": "us-east-1c",
                        "GroupName": "HDFS-Group-A",
                        "PartitionNumber": 7,
                        "Tenancy": "default"
                    }

                {
                    "InstanceId": "i-0a9b876cd5d4ef321",
                    "InstanceType": "r4.large",
                    },

                    "Placement": {
                        "AvailabilityZone": "us-east-1c",
                        "GroupName": "HDFS-Group-A",
                        "PartitionNumber": 7,
                        "Tenancy": "default"
                    }
            ],
```

Cambiar el grupo de ubicación para una instancia

Puede cambiar el grupo con ubicación de una instancia de la siguiente manera:

- Puede mover una instancia existente a un grupo de ubicación
- Puede mover una instancia de un grupo de ubicación a otro

Para poder mover la instancia, esta debe estar en estado `stopped`.

Console

Mover una instancia a un grupo con ubicación

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Seleccione la instancia y luego elija Estado de la instancia, Detener instancia.
4. Con la instancia aún seleccionada, elija Acciones, Configuración de la instancia, Cambiar ubicación de la instancia.
5. En Grupo con ubicación, seleccione el grupo con ubicación al cual se moverá la instancia.
6. Seleccione Guardar.

AWS CLI

Mover una instancia a un grupo con ubicación

1. Detenga la instancia con el comando stop-instances.
2. Use el comando modify-instance-placement y especifique el nombre del grupo con ubicación al cual se moverá la instancia.

```
aws ec2 modify-instance-placement \
    --instance-id i-0123a456700123456 \
    --group-name MySpreadGroup
```

3. Inicie la instancia con el comando start-instances.

PowerShell

Para mover una instancia a un grupo de ubicación utilizando la AWS Tools for Windows PowerShell

1. Detenga la instancia con el comando Stop-EC2Instance.

2. Utilice el comando Edit-EC2InstancePlacement y especifique el nombre del grupo de ubicación al que desea mover la instancia.
3. Inicie la instancia con el comando Start-EC2Instance.

Puede quitar una instancia de un grupo de ubicación

Puede eliminar una instancia de un grupo con ubicación mediante uno de los siguientes métodos.

Para poder quitar una instancia de un grupo con ubicación, la instancia debe estar en estado `stopped`.

Console

Quitar una instancia de un grupo con ubicación

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Seleccione la instancia y luego elija Estado de la instancia, Detener instancia.
4. Con la instancia aún seleccionada, elija Acciones, Configuración de la instancia, Cambiar ubicación de la instancia.
5. En Grupo con ubicación, elija Ninguno.
6. Seleccione Guardar.

AWS CLI

Quitar una instancia de un grupo con ubicación

1. Detenga la instancia con el comando stop-instances.
2. Utilice el comando modify-instance-placement y especifique una cadena vacía para el nombre del grupo de ubicación.

```
aws ec2 modify-instance-placement \
    --instance-id i-0123a456700123456 \
    --group-name ""
```

3. Inicie la instancia con el comando start-instances.

PowerShell

Para quitar una instancia de un grupo de ubicación utilizando la AWS Tools for Windows PowerShell

1. Detenga la instancia con el comando Stop-EC2Instance.
2. Utilice el comando Edit-EC2InstancePlacement y especifique una cadena vacía para el nombre del grupo de ubicación.
3. Inicie la instancia con el comando Start-EC2Instance.

Eliminar un grupo de ubicación

Si necesita reemplazar un grupo de ubicación o si ya no lo necesita, puede eliminarlo. Para eliminar un grupo de ubicación, utilice uno de los métodos siguientes.

Requisito previo

Para que un grupo de ubicación pueda eliminarse, no debe contener instancias. Puede terminar todas las instancias que lanzó en el grupo con ubicación, moverlas a otro grupo con ubicación o eliminarlas del grupo con ubicación.

Console

Eliminar un grupo con ubicación

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Grupos de ubicación.
3. Seleccione el grupo de ubicación y elija Acciones, Eliminar.
4. Cuando le pidan confirmación, escriba **`Delete`** y elija Eliminar.

AWS CLI

Eliminar un grupo con ubicación

Utilice el comando delete-placement-group y especifique el nombre del grupo de ubicación para eliminarlo. En este ejemplo, el nombre del grupo de ubicación es `my-cluster`.

```
aws ec2 delete-placement-group --group-name my-cluster
```

PowerShell

Para eliminar un grupo de ubicación con la AWS Tools for Windows PowerShell

Utilice el comando Remove-EC2PlacementGroup para eliminar el grupo de colocación.

Compartir un grupo con ubicación

El uso compartido de grupos con ubicación le permite influir en la ubicación de instancias interdependientes que pertenecen a cuentas independientes de AWS. Puede compartir un grupo con ubicación en varias cuentas de AWS o en su organización. Puede iniciar instancias en un grupo con ubicación compartido.

El propietario de un grupo con ubicación puede compartir un grupo con ubicación con:

- Cuentas específicas de AWS dentro o fuera de su organización
- Una unidad organizativa dentro de su organización de
- Toda su organización de

> **Note**
>
> La cuenta de AWS desde la que desea compartir un grupo con ubicación debe tener los siguientes permisos en la política de IAM.
>
> - `ec2:PutResourcePolicy`
> - `ec2:DeleteResourcePolicy`

Temas

Reglas y limitaciones

Las siguientes reglas y limitaciones se aplican cuando comparte un grupo con ubicación o cuando se comparte uno con usted.

- Para compartir un grupo con ubicación, debe tenerlo en su cuenta de AWS. No puede compartir un grupo con ubicación que se haya compartido con usted.
- Cuando se comparte un grupo con ubicación distribuida o en particiones, los límites del grupo con ubicación no cambian. Un grupo con ubicación en particiones compartido admite un máximo de siete particiones por zona de disponibilidad, y un grupo con ubicación distribuida compartido admite un máximo de siete instancias en ejecución por zona de disponibilidad.
- Para compartir un grupo con ubicación con su organización o una unidad organizativa de la organización, debe habilitar el uso compartido con AWS Organizations. Para obtener más información, consulte Uso compartido de los recursos de AWS.
- Es responsable de administrar las instancias de su propiedad en un grupo con ubicación compartido.
- No puede ver ni modificar instancias ni reservas de capacidad que estén asociadas a un grupo con ubicación compartido, pero que no sean de su propiedad.

Compartir el uso entre zonas de disponibilidad

Para garantizar que los recursos se distribuyen por todas las zonas de disponibilidad de una región, asignamos zonas de disponibilidad de manera independiente a nombres de cada cuenta. Esto podría dar lugar a diferencias de nomenclatura de zona de disponibilidad entre cuentas. Por ejemplo, es posible que la zona de disponibilidad `us-east-1a` de su cuenta de AWS no se encuentre en la misma ubicación de `us-east-1a` que otra cuenta de AWS.

Para identificar la ubicación de los hosts dedicados relativa a las cuentas, debe utilizar el ID de zona de disponibilidad (ID de AZ). El ID de zona de disponibilidad es un identificador único e idéntico para una zona de disponibilidad en todas las cuentas de AWS. Por ejemplo, `use1-az1` es un ID de zona de disponibilidad para la región `us-east-1` y está en la misma ubicación en todas las cuentas de AWS.

Para ver los ID de zona de disponibilidad de las zonas de disponibilidad de su cuenta

1. Abra la consola de AWS RAM en https://console.aws.amazon.com/ram.

2. Los ID de zona de disponibilidad de la región actual se muestran en Su ID de zona de disponibilidad, en el panel derecho.

Compartir un grupo con ubicación

Para compartir un grupo con ubicación, debe agregarlo a un recurso compartido. Un uso compartido de recursos es un recurso de AWS RAM que le permite compartir los recursos a través de cuentas de AWS. Un uso compartido de recursos especifica los recursos que compartir y los consumidores con quienes se comparten.

Si forma parte de una organización en AWS Organizations, está habilitado el uso compartido dentro de su organización y se otorga a los consumidores de su organización acceso al grupo con ubicación compartido.

Si el grupo con ubicación se comparte con una cuenta de AWS ajena a su organización, el propietario de la cuenta de AWS recibirá una invitación para unirse al recurso compartido. Podrán acceder al grupo con ubicación compartido después de aceptar la invitación.

Puede compartir un grupo con ubicación entre cuentas de AWS mediante https://console.aws.amazon.com/ram o la AWS CLI.

AWS RAM console

Para compartir un grupo con ubicación de su propiedad mediante https://console.aws.amazon.com/ram, consulte Crear un recurso compartido.

AWS CLI

Para compartir un grupo con ubicación de su propiedad, use el comando create-resource-share.

Identificar un grupo con ubicación compartido

El nombre de recurso de Amazon (ARN) de un grupo con ubicación contiene el ID de 12 dígitos de la cuenta propietaria del grupo con ubicación. Puede utilizar el ID de la cuenta para identificar al propietario de un grupo con ubicación compartido con usted.

Puede encontrar el ARN del grupo con ubicación mediante uno de los siguientes métodos. Para obtener más información, consulte Visualización de información de los grupos con ubicación.

Amazon EC2 console

Para identificar un grupo con ubicación compartido

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Red y seguridad, seleccione Grupos de ubicación.
3. En la tabla Grupos de ubicación se enumeran todos los grupos con ubicación de su propiedad y compartidos con usted. En la columna ARN del grupo se muestra el ARN del grupo con ubicación.

   Si la columna ARN del grupo no está visible, seleccione la configuración () en la esquina superior derecha, active ARN del grupo y, a continuación, seleccione Confirmar.

AWS CLI

Para identificar un grupo con ubicación compartido

Utilice el comando `describe-placement-groups` para mostrar todos los grupos con ubicación de su propiedad y compartidos con usted. En la respuesta, el parámetro `GroupId` muestra el ARN de un grupo con ubicación.

Iniciar una instancia en un grupo con ubicación compartido

> **Important**
>
> Cuando utilice la AWS CLI para iniciar una instancia en un grupo con ubicación compartido, debe especificar el ID del grupo con ubicación mediante el parámetro `GroupId`.

Puede usar el nombre del grupo con ubicación solo si es el propietario del grupo con ubicación que se comparte. Recomendamos utilizar el ID del grupo con ubicación para evitar posibles conflictos de nombres de grupos con ubicación entre cuentas de AWS.

Puede encontrar el ID de un grupo con ubicación en la consola de Amazon EC2, en la pantalla Grupos de ubicación o mediante el comando `describe-placement-groups` de la AWS CLI. Para obtener más información, consulte Visualización de información de los grupos con ubicación.

Console

Para iniciar instancias en un grupo con ubicación compartido

1. Siga el procedimiento para iniciar una instancia, pero no la lance hasta que haya completado los siguientes pasos para especificar la configuración del grupo con ubicación.
2. En Tipo de instancia, elija un tipo de instancia admitido. Para obtener más información, consulte Reglas y limitaciones de los grupos de ubicación.
3. Amplíe la sección Detalles avanzados y configure de la siguiente manera los ajustes del grupo con ubicación:

   a. En Grupo de ubicación, seleccione el que se compartió con usted.

   > **Note**
   >
   > Si hay grupos con ubicación que tengan el mismo nombre, compruebe el ID del grupo con ubicación para asegurarse de que haya seleccionado el correcto.

   b. Si elige un grupo con ubicación con una estrategia de partición, en Partición de destino, elija la partición en la que quiera iniciar la instancia.
4. En el panel Resumen, haga lo siguiente:

   a. Para Número de instancias, introduzca el número total de instancias que necesita en este grupo de ubicación, ya que es posible que más adelante no pueda añadirle más instancias.

   b. Revise la configuración de la instancia y, a continuación, elija iniciar instancia.

Para obtener más información, consulte Lance una instancia con el nuevo asistente de inicialización de instancias.

AWS CLI

Para iniciar instancias en un grupo con ubicación compartido

Utilice el comando `run-instances` y especifique el ID del grupo con ubicación compartido.

```
aws ec2 run-instances –-placement "GroupId = pg-0123456789example"
```

Para iniciar instancias en una partición específica de un grupo con ubicación en particiones compartido

Utilice el comando `run-instances` y especifique el ID del grupo con ubicación y el número de partición del grupo con ubicación compartido.

```
aws ec2 run-instances –-placement "GroupId = pg-0123456789example, PartitionNumber
 = 3"
```

> **Tip**
>
> Utilice la interconexión de VPC para conectar instancias que pertenezcan a cuentas independientes de AWS y aprovechar todos los beneficios de latencia que ofrecen los grupos con ubicación en clúster compartidos. Para obtener más información, consulte ¿Qué es un emparejamiento de VPC?

Dejar de compartir un grupo con ubicación compartido

El propietario del grupo con ubicación puede dejar de compartir un grupo con ubicación compartido en cualquier momento.

Al anular el uso compartido de un grupo con ubicación compartido, se aplicarán los siguientes cambios.

- Las cuentas de AWS con las que se compartió un grupo con ubicación ya no podrán iniciar instancias ni reservar capacidad.
- Si sus instancias se ejecutaban en un grupo con ubicación compartido, se desasociarán del grupo con ubicación, pero seguirán ejecutándose con normalidad en su cuenta de AWS.
- Si tenía reservas de capacidad en un grupo de ubicación compartido, se desasociarán del grupo con ubicación, pero seguirá teniendo acceso a ellas en su cuenta de AWS.

Puede anular el uso compartido de un grupo con ubicación mediante uno de los siguientes métodos.

AWS RAM console

Para dejar de compartir un grupo con ubicación compartido mediante https://console.aws.amazon.com/ram, consulte Eliminar un recurso compartido.

AWS CLI

Para dejar de compartir un grupo con ubicación compartido mediante AWS Command Line Interface, utilice el comando disassociate-resource-share.

Grupos de ubicación en AWS Outposts

AWS Outposts es un servicio completamente administrado que extiende la infraestructura, los servicios, las API y las herramientas de AWS a las instalaciones del cliente. Al proporcionar acceso local a la infraestructura administrada de AWS, AWS Outposts habilita a los clientes a crear y ejecutar aplicaciones en las instalaciones mediante el uso de las mismas interfaces de programación que en las regiones de AWS, al mismo tiempo que utilizan recursos informáticos y de almacenamiento locales para reducir la latencia y las necesidades de procesamiento de datos locales.

Un Outpost es un grupo de capacidad informática y de almacenamiento de AWS implementada en un sitio del cliente. AWS opera, supervisa y administra esta capacidad como parte de una región de AWS.

Puede crear grupos de ubicación en Outposts que haya creado en su cuenta. Esto le permite distribuir instancias en el equipo subyacente en un Outpost en su sitio. Los grupos de ubicación en Outposts se crean y usan de la misma manera que se crean y usan los grupos de ubicación en zonas de disponibilidad normales. Cuando crea un grupo de ubicación con una estrategia de distribución en Outpost, puede elegir que el grupo de ubicación distribuya instancias entre hosts o bastidores. Distribuir instancias entre hosts le permite usar una estrategia de distribución con un Outpost de un solo bastidor.

Consideraciones

- Un grupo con ubicación distribuida de bastidor puede contener tantas instancias como bastidores tenga en su implementación de Outpost.
- Un grupo con ubicación distribuida de host puede contener tantas instancias como hosts tenga en su implementación de Outpost.

Requisito previo

Debe tener un Outpost instalado en su sitio. Para obtener más información, consulte Crear una instancia de Outpost y solicitar capacidad de Outpost en la Guía del usuario de AWS Outposts.

Para usar un grupo de ubicación en Outpost

1. Cree una subred en el Outpost. Para obtener más información, consulte Crear una subred en la Guía del usuario de AWS Outposts.
2. Cree un grupo de ubicación en la región asociada de Outpost. Si crea un grupo con ubicación con una estrategia de distribución, puede elegir la distribución de host o bastidor para determinar cómo distribuirá el grupo las instancias por todo el hardware subyacente en su Outpost. Para obtener más información, consulte the section called “Crear un grupo de ubicación”.
3. Inicie una instancia en un grupo de ubicación. En Subred, elija la subred que creó en el paso 1, y para Nombre del grupo de ubicación, seleccione el grupo de ubicación que creó en el paso 2. Para obtener más información, consulte iniciar una instancia en Outpost en la Guía del usuario de AWS Outposts.

Unidad de transmisión máxima (MTU) de red de la instancia de EC2

La unidad de transmisión máxima (MTU) de una conexión de red es el tamaño, en bytes, del mayor paquete permitido que se puede transferir a través de la conexión. Cuanto mayor sea la MTU de una conexión, mayor cantidad de datos se podrán transferir en un solo paquete. Los marcos Ethernet consisten del packet, o los datos que está enviando, y de la información de sobrecarga de red que lo rodea.

Las tramas Ethernet pueden presentar distintos formatos, siendo el más habitual de ellos el formato de tramas estándar Ethernet v2. Admite 1500 MTU, que es el mayor tamaño de paquete Ethernet admitido por la mayor parte de aplicaciones de Internet. La MTU admitida para una instancia depende del tipo de instancia.

Las siguientes reglas se aplican a las instancias que se encuentran en zonas de Wavelength:

- El tráfico que va de una instancia a otra dentro de una VPC en la misma zona de Wavelength tiene una MTU de 1300.
- El tráfico que va de una instancia a otra que utiliza la IP del operador dentro de una zona de Wavelength tiene una MTU de 1500.
- El tráfico que va de una instancia a otra entre una zona de Wavelength y la región que utiliza una dirección IP pública tiene una MTU de 1500.

- El tráfico que va de una instancia a otra entre una zona de Wavelength y la región que utiliza una dirección IP privada tiene una MTU de 1300.

Las siguientes reglas se aplican a las instancias que se encuentran en Outposts:

- El tráfico que va de una instancia en Outposts a una instancia en la región tiene una MTU de 1300.

Contenido

Tramas gigantes (9 001 MTU)

Las tramas gigantes permiten más de 1500 bytes de datos al aumentar el tamaño de la carga por paquete, incrementando así el porcentaje del paquete que no supone una sobrecarga del mismo. De este modo, se necesitan menos paquetes para enviar la misma cantidad de datos utilizables. Sin embargo, el tráfico está limitado a una MTU máxima de 1500 en los siguientes casos:

- Tráfico a través de una NAT puerta de enlace de Internet
- Tráfico a través de una interconexión de VPC entre regiones
- Tráfico a través de conexiones de VPN
- Tráfico fuera de una región de AWS determinada

Si los paquetes tienen más de 1500 bytes, se fragmentan o, si se establece la marca `Don't Fragment` en el encabezado IP, se eliminan.

Las tramas gigantes se deben utilizar con precaución para el tráfico vinculado a Internet o cualquier tráfico que salga de una VPC. Los paquetes son fragmentados por sistemas intermedios, lo que ralentiza el tráfico. Para utilizar tramas gigantes dentro de una VPC y no ralentizar el tráfico que se dirige fuera de la misma, puede configurar el tamaño de la MTU por ruta o bien utilizar varias interfaces de red elásticas con diferentes tamaños de MTU y diferentes rutas.

En el caso de las instancias que se colocan dentro de un grupo con ubicación en clúster, se recomienda usar tramas gigantes, que ayudan a obtener el máximo rendimiento de red posible. Para obtener más información, consulte Grupos de ubicación.

Puede utilizar tramas gigantes para el tráfico entre las VPC y las redes locales a través de AWS Direct Connect. Para obtener más información y para saber cómo verificar la capacidad de tramas gigantes, consulte Cómo configurar la MTU de red en la Guía del usuario de AWS Direct Connect.

Todos los tipos de instancias de Amazon EC2 admiten 1500 MTU y todos los tipos de instancias de la generación actual admiten tramas gigantes. Los siguientes tipos de instancias de la generación anterior también admiten tramas gigantes: A1, C3, I2, M3, y R3.

Para obtener más información sobre los tamaños de MTU compatibles:

- Para las puertas de enlace de NAT, consulte Conceptos básicos de las puertas de enlace de NAT en la Guía del usuario de Amazon VPC.
- Para las puertas de enlace de tránsito, consulte MTU en la Guía del usuario de puertas de enlace de tránsito de Amazon VPC.
- Para zonas locales, consulte Consideraciones en la Guía del usuario de zonas locales de AWS.

Detección de la MTU de la ruta

La detección de la MTU de la ruta (PMTUD) se utiliza para determinar la MTU de la ruta entre dos dispositivos. La MTU de la ruta es tamaño máximo del paquete admitido en la ruta entre el host de origen y el host receptor. Cuando hay una diferencia en el tamaño de la MTU en la red entre los dos hosts, PMTUD permite que el host receptor responda al host de origen con un mensaje ICMP. Este mensaje de ICMP indica al host de origen que utilice el mínimo tamaño de la MTU en la ruta de la red para volver a enviar la solicitud. Sin esta negociación, puede perderse el paquete porque la solicitud es muy grande para que la acepte el host receptor.

Para IPv4, cuando un host envía un paquete mayor que la MTU del host receptor o que es mayor que la MTU de un dispositivo a lo largo de la ruta, el host o dispositivo receptor descarta el paquete y, a continuación, devuelve el siguiente mensaje ICMP: `Destination Unreachable: Fragmentation Needed and Don't Fragment was Set` (Tipo 3, código 4). Esto indica al host transmisor que divida la carga útil en varios paquetes más pequeños y, a continuación, los retransmita.

El protocolo IPv6 no admite la fragmentación en la red. Cuando un host envía un paquete mayor que la MTU del host receptor o que es mayor que la MTU de un dispositivo a lo largo de la ruta, el host

o dispositivo receptor descarta el paquete y, a continuación, devuelve el siguiente mensaje ICMP: `ICMPv6 Packet Too Big (PTB)` (Tipo 2). Esto indica al host transmisor que divida la carga útil en varios paquetes más pequeños y, a continuación, los retransmita.

Las conexiones realizadas a través de algunos componentes, como las puertas de enlace de NAT y los equilibradores de carga, se rastrean automáticamente. Esto significa que el seguimiento de grupos de seguridad está habilitado de forma automática para los intentos de conexión saliente. Si las conexiones se rastrean automáticamente o si las reglas de su grupo de seguridad permiten el tráfico ICMP entrante, puede recibir respuestas de PMTUD.

Tenga en cuenta que el tráfico ICMP se puede bloquear incluso si está permitido a nivel de grupo de seguridad, por ejemplo, si tiene una entrada en la lista de control de acceso a la red que deniega el tráfico ICMP a la subred.

> **Important**
>
> La detección de MTU de ruta no garantiza que algunos enrutadores no eliminen tramas gigantes. Una puerta de enlace de Internet en la VPC reenviará los paquetes solo hasta los 1500 bytes. Para el tráfico de internet se recomiendan paquetes de 1500 MTU.

Comprobar la MTU de la ruta entre dos hosts

Puede comprobar la MTU de la ruta entre la instancia EC2 y otro host. Puede especificar un nombre de DNS o una dirección IP como destino. Si el destino es otra instancia EC2, verifique que el grupo de seguridad permita el tráfico de UDP entrante.

El procedimiento que utiliza depende del sistema operativo de la instancia.

instancias de Linux

Ejecute el comando tracepath en la instancia para comprobar la MTU de la ruta entre la instancia EC2 y el destino especificado. Este comando forma parte del paquete `iputils`, que está disponible de forma predeterminada en muchas distribuciones de Linux.

En este ejemplo se comprueba la MTU de la ruta entre la instancia EC2 y `amazon.com`.

```
[ec2-user ~]$ tracepath amazon.com
```

En esta salida de ejemplo, la MTU de la ruta es 1500.

```
 1?: [LOCALHOST]     pmtu 9001
 1:  ip-172-31-16-1.us-west-1.compute.internal (172.31.16.1)   0.187ms pmtu 1500
 1:  no reply
 2:  no reply
 3:  no reply
 4:  100.64.16.241 (100.64.16.241)                              0.574ms
 5:  72.21.222.221 (72.21.222.221)                             84.447ms asymm 21
 6:  205.251.229.97 (205.251.229.97)                           79.970ms asymm 19
 7:  72.21.222.194 (72.21.222.194)                             96.546ms asymm 16
 8:  72.21.222.239 (72.21.222.239)                             79.244ms asymm 15
 9:  205.251.225.73 (205.251.225.73)                           91.867ms asymm 16
...
31:  no reply
     Too many hops: pmtu 1500
     Resume: pmtu 1500
```

instancias de Windows

Para comprobar la MTU de la ruta con mturoute

1. Descargue mturoute.exe en su instancia EC2 desde http://www.elifulkerson.com/projects/mturoute.php.
2. Abra una ventana del símbolo del sistema y cambie al directorio en el que haya descargado mturoute.exe.
3. Utilice el siguiente comando para comprobar la MTU de la ruta entre la instancia EC2 y el destino especificado. En este ejemplo se comprueba la MTU de la ruta entre la instancia EC2 y `www.elifulkerson.com`.

   ```
   .\mturoute.exe www.elifulkerson.com
   ```

   En esta salida de ejemplo, la MTU de la ruta es 1500.

   ```
   * ICMP Fragmentation is not permitted. *
   * Speed optimization is enabled. *
   * Maximum payload is 10000 bytes. *
   + ICMP payload of 1472 bytes succeeded.
   - ICMP payload of 1473 bytes is too big.
   Path MTU: 1500 bytes.
   ```

Comprobación de la MTU de la instancia

Puede comprobar el valor de la MTU de la instancia. Algunas instancias están configuradas para utilizar tramas gigantes y otras están configuradas para utilizar tamaños de trama estándar.

El procedimiento que utiliza depende del sistema operativo de la instancia.

instancias de Linux

Para comprobar la configuración de la MTU de una instancia Linux

Ejecute el siguiente comando ip en la instancia EC2. Si la interfaz de red principal no es `eth0`, sustituya `eth0` por la interfaz de red.

```
[ec2-user ~]$ ip link show eth0
```

En la salida del ejemplo, *`mtu 9001`* indica que esta instancia utiliza tramas gigantes.

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP mode
 DEFAULT group default qlen 1000
    link/ether 02:90:c0:b7:9e:d1 brd ff:ff:ff:ff:ff:ff
```

instancias de Windows

El procedimiento que utiliza depende del controlador de su instancia.

ENA driver

Versión 2.1.0 y posteriores

Para obtener el valor de la MTU, use el siguiente comando Get-NetAdapterAdvancedProperty en la instancia EC2. Utilice el comodín (asterisco) para obtener todos los nombres de Ethernet. Compruebe la salida correspondiente al nombre de interfaz `*JumboPacket`. Un valor de 9015 indica que las tramas gigantes están habilitadas. Las tramas gigantes están deshabilitadas de forma predeterminada.

```
Get-NetAdapterAdvancedProperty -Name "Ethernet*"
```

Versión 1.5 y anteriores

Para obtener el valor de la MTU, use el siguiente comando Get-NetAdapterAdvancedProperty en la instancia EC2. Compruebe la salida correspondiente al nombre de interfaz `MTU`. Un valor de

9001 indica que las tramas gigantes están habilitadas. Las tramas gigantes están deshabilitadas de forma predeterminada.

```
Get-NetAdapterAdvancedProperty -Name "Ethernet"
```

Intel SRIOV 82599 driver

Para obtener el valor de la MTU, use el siguiente comando Get-NetAdapterAdvancedProperty en la instancia EC2. Compruebe la entrada correspondiente al nombre de interfaz `*JumboPacket`. Un valor de 9014 indica que las tramas gigantes están habilitadas. (Tenga en cuenta que el tamaño de la MTU incluye el encabezado y la carga). Las tramas gigantes están deshabilitadas de forma predeterminada.

```
Get-NetAdapterAdvancedProperty -Name "Ethernet"
```

AWS PV driver

Para obtener el valor de la MTU, use el siguiente comando en la instancia EC2. El nombre de la interfaz puede variar. En la salida, busque una entrada llamada "Ethernet", "Ethernet 2" o "Local Area Connection". Necesita el nombre de la interfaz para habilitar y para deshabilitar las tramas gigantes. Un valor de 9001 indica que las tramas gigantes están habilitadas.

```
netsh interface ipv4 show subinterface
```

Configuración de la MTU de la instancia

Es posible que desee utilizar tramas gigantes para el tráfico de red dentro de la VPC y tramas estándar para el tráfico de Internet. Sea cual sea el caso de uso, le recomendamos que verifique que su instancia se comporte según lo previsto.

El procedimiento que utiliza depende del sistema operativo de la instancia.

instancias de Linux

Para establecer el valor de la MTU con una instancia de Linux

1. Ejecute el siguiente comando ip en la instancia. Establece el valor deseado de la MTU en 1500, pero también puede utilizar un valor de 9001.

```
[ec2-user ~]$ sudo ip link set dev eth0 mtu 1500
```

2. (Opcional) Para que la configuración de la MTU de la red persista tras un reinicio, modifique los siguientes archivos de configuración, en función del tipo de sistema operativo que use.

   - Para Amazon Linux 2, añada la línea siguiente al archivo `/etc/sysconfig/network-scripts/ifcfg-eth0`:

     ```
     MTU=1500
     ```

     Añada la línea siguiente al archivo `/etc/dhcp/dhclient.conf`:

     ```
     request subnet-mask, broadcast-address, time-offset, routers, domain-name,
      domain-search, domain-name-servers, host-name, nis-domain, nis-servers, ntp-
     servers;
     ```

   - Para la AMI de Amazon Linux, añada las siguientes líneas al archivo `/etc/dhcp/dhclient-eth0.conf`.

     ```
     interface "eth0" {
     supersede interface-mtu 1500;
     }
     ```

   - Para otras distribuciones Linux, consulte la documentación específica.

3. (Opcional) Reinicie la instancia y compruebe que la configuración de la MTU sea correcta.

instancias de Windows

El procedimiento que utiliza depende del controlador de su instancia.

ENA driver

Para cambiar la MTU, utilice el administrador de dispositivos o el comando Set-NetAdapterAdvancedProperty en la instancia.

Versión 2.1.0 y posteriores

Utilice el siguiente comando para activar tramas gigantes.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -
RegistryValue 9015
```

Utilice el siguiente comando para desactivar tramas gigantes.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -
RegistryValue 1514
```

Versión 1.5 y anteriores

Utilice el siguiente comando para activar tramas gigantes.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "MTU" -
RegistryValue 9001
```

Utilice el siguiente comando para desactivar tramas gigantes.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "MTU" -
RegistryValue 1500
```

Intel SRIOV 82599 driver

Para cambiar la MTU, utilice el administrador de dispositivos o el comando Set-NetAdapterAdvancedProperty en la instancia.

Utilice el siguiente comando para activar tramas gigantes.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -
RegistryValue 9014
```

Utilice el siguiente comando para desactivar tramas gigantes.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -
RegistryValue 1514
```

AWS PV driver

Puede cambiar la MTU con el comando netsh en la instancia. No puede cambiar la MTU con el administrador de dispositivos.

Utilice el siguiente comando para activar tramas gigantes.

```
netsh interface ipv4 set subinterface "Ethernet" mtu=9001
```

Utilice el siguiente comando para desactivar tramas gigantes.

```
netsh interface ipv4 set subinterface "Ethernet" mtu=1500
```

Solución de problemas

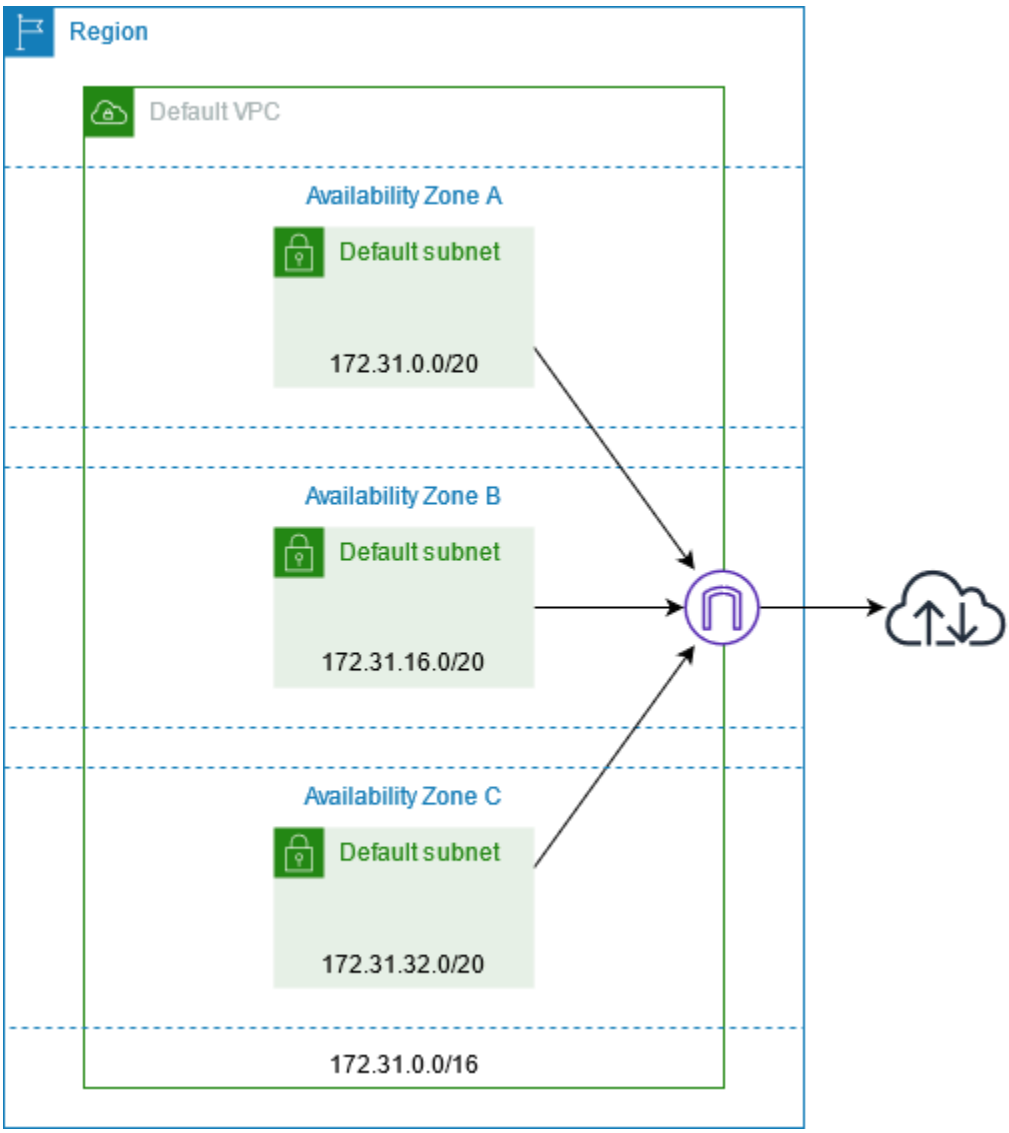
Si experimenta problemas de conectividad entre la instancia EC2 y un clúster de Amazon Redshift al utilizar tramas gigantes, consulte Falta de respuesta de las consultas en la Guía de administración de Amazon Redshift.

Nubes privadas virtuales para sus instancias EC2

Amazon Virtual Private Cloud (Amazon VPC) le permite definir una red virtual en su propia área aislada lógicamente dentro de la nube de AWS, conocida como nube virtual privada o VPC. Puede crear recursos de AWS, como instancias de Amazon EC2, en las subredes de su VPC. La VPC es prácticamente idéntica a una red tradicional que usted puede utilizar en su propio centro de datos, con los beneficios que supone utilizar la infraestructura escalable de AWS. Puede configurar la VPC, seleccionar su rango de direcciones IP, crear subredes y configurar tablas de enrutamiento, puerta de enlace de red y ajustes de seguridad. Puede conectar instancias de la VPC a Internet o a su propio centro de datos.

Sus VPC predeterminadas

Cuando cree su cuenta de AWS, crearemos automáticamente una VPC predeterminada en cada región. Una VPC predeterminada es aquella que ya está configurada y se puede utilizar. Por ejemplo, hay una subred predeterminada para cada zona de disponibilidad de cada VPC predeterminada, una puerta de enlace de Internet conectada a la VPC y una ruta en la tabla de enrutamiento principal que envía todo el tráfico (0.0.0.0/0) a la puerta de enlace de Internet. También puede crear su propia VPC y configurarla en función de sus necesidades.



Crear VPC adicionales

Utilice el siguiente procedimiento para crear una VPC con la configuración de subredes, puertas de enlace y enrutamiento que necesite.

Para crear una VPC

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. Seleccione Crear VPC.
3. En Recursos para crear elija VPC y más.
4. En Generación automática de etiquetas de nombre, ingrese un nombre para la VPC.

5. En Bloque CIDR de IPv4, conserve la sugerencia predeterminada e ingrese el bloque CIDR necesario para su aplicación o red.
6. En Número de zonas de disponibilidad, elija 2 para poder iniciar instancias en varias zonas de disponibilidad y garantizar una alta disponibilidad.
7. Si se debe acceder a las instancias desde Internet, haga una de las siguientes operaciones:
   - Si las instancias pueden estar en una subred pública, seleccione un valor que no sea cero en Cantidad de subredes públicas. Mantenga ambas opciones seleccionadas en Opciones de DNS. Si lo desea, puede agregar subredes privadas ahora o más adelante.
   - Si las instancias deben estar en una subred privada, seleccione 0 en Cantidad de subredes públicas. En Número de subredes privadas, seleccione un número según sus necesidades (los valores posibles corresponden a 1 o 2 subredes privadas por zona de disponibilidad). En Puertas de enlace NAT, si las instancias de ambas zonas de disponibilidad envían o reciben un volumen significativo de tráfico a través de ellas, seleccione 1 por AZ. De lo contrario, seleccione En 1 AZ y lance instancias que envíen o reciban tráfico entre zonas en la misma zona de disponibilidad que la puerta de enlace NAT.
8. Expanda Personalizar bloques CIDR de subred. Conserve las sugerencias predeterminadas o introduzca un bloque CIDR para cada subred. Para obtener más información, consulte bloques CIDR de subred en la Guía del usuario de Amazon VPC.
9. Revise el panel Vista previa, que muestra los recursos de VPC que se crearán en función de las selecciones.
10. Seleccione Crear VPC.

Acceso a Internet desde sus instancias

Las instancias iniciadas en una subred predeterminada en una VPC predeterminada tienen acceso a Internet, ya que las VPC predeterminadas están configuradas para asignar direcciones IP públicas y nombres de host DNS y la tabla de enrutamiento principal se configura con una ruta a una puerta de enlace de Internet conectada a la VPC.

Para las instancias que lance en subredes y VPC no predeterminadas, puede utilizar uno de las siguientes opciones para asegurarse de que las instancias que lance en estas subredes tengan acceso a Internet:

- Configure una puerta de enlace de Internet. Para obtener más información, consulte Conectar subredes a Internet por medio de una puerta de enlace de Internet en la Guía del usuario de Amazon VPC.

- Configure una puerta de enlace de NAT pública. Para obtener más información, consulte Acceso a Internet desde una subred privada en la Guía del usuario de Amazon VPC.

Subredes compartidas

Al iniciar instancias de EC2 en subredes de VPC compartidas, tenga en cuenta lo siguiente:

- Los participantes pueden ejecutar instancias en una subred compartida al especificar el ID de la subred compartida. Los participantes deben ser propietarios de los grupos de seguridad o las interfaces de red que especifiquen.
- Los participantes pueden iniciar, detener, finalizar y describir las instancias que crearon en una subred compartida. Los participantes no pueden iniciar, detener, finalizar o describir las instancias creadas por el propietario de una VPC en una subred compartida.
- Los propietarios de VPC no pueden iniciar, detener, finalizar o describir las instancias creadas por los participantes en una subred compartida.
- Los participantes pueden conectarse a una instancia de una subred compartida con el punto de conexión de EC2 Instance Connect. El participante debe crear el punto de conexión de EC2 Instance Connect en la subred compartida. Los participantes no pueden utilizar un punto de conexión de EC2 Instance Connect creada por el propietario de la VPC en la subred compatida.

Para obtener más información, consulte Compartir su VPC con otras cuentas en la Guía del usuario de Amazon VPC.

Subredes solo de IPv6

Una instancia de EC2 iniciada en una subred de solo IPv6 recibe una dirección IPv6, pero no una dirección IPv4. Todas las instancias que inicialice en una subred sólo IPv6 deben ser instancias integradas en el AWS Nitro System.

Seguridad en Amazon EC2

La seguridad en la nube de AWS es la mayor prioridad. Como cliente de AWS, se beneficiará de una arquitectura de red y un centro de datos que están diseñados para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

La seguridad es una responsabilidad compartida entre AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWSes responsable de proteger la infraestructura que ejecuta los servicios de AWS en la nube de AWS. AWS también proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los Programas de conformidad de AWS . Para obtener información sobre los programas de conformidad que se aplican a Amazon EC2, consulte Servicios de AWS en el ámbito del programa de conformidad.
- Seguridad en la nube – las siguientes áreas son su responsabilidad:
  - Control del acceso de la red a las instancias, por ejemplo, mediante la configuración de la VPC y los grupos de seguridad. Para obtener más información, consulte Control del tráfico de red.
  - Gestión de las credenciales utilizadas para conectarse a las instancias.
  - Gestión del sistema operativo invitado y el software implementado en dicho sistema, que abarca actualizaciones y parches de seguridad. Para obtener más información, consulte Administración de actualizaciones para instancias de Windows de Amazon EC2.
  - Configuración de los roles de IAM que están asociados a la instancia y los permisos vinculados con esos roles. Para obtener más información, consulte Roles de IAM para Amazon EC2.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza Amazon EC2. Muestra cómo configurar Amazon EC2 para satisfacer sus objetivos de seguridad y conformidad. También puede aprender a utilizar otros servicios de AWS que ayudan a monitorear y proteger los recursos de Amazon EC2.

Contenido

- Identity and Access Management para Amazon EC2
- Acceso a Amazon EC2 mediante un punto de conexión de VPC de interfaz.
- Administración de actualizaciones para instancias de Windows de Amazon EC2
- Prácticas recomendadas de seguridad para instancias de Windows
- Pares de claves e instancias de Amazon EC2
- Grupos de seguridad de Amazon EC2 para instancias EC2
- NitroTPM
- Credential Guard para instancias de Windows

Proteger los datos en Amazon EC2

El modelo de responsabilidad compartida de AWS se aplica a la protección de datos en Amazon Elastic Compute Cloud (EC2). Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta toda la Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS.

Con fines de protección de datos, recomendamos proteger las credenciales de la Cuenta de AWS y configurar cuentas de usuario individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos de AWS. Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure los registros de API y de actividad de los usuarios con AWS CloudTrail.
- Utilice las soluciones de cifrado de AWS, junto con todos los controles de seguridad predeterminados dentro de los servicios de Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.

- Si necesita módulos criptográficos validados FIPS 140-2 al acceder a AWS a través de una interfaz de línea de comandos o una API, utilice un punto de conexión de FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como, por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con Amazon EC2 u otros Servicios de AWS mediante la consola, la API, la AWS CLI o los AWS SDK. Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Contenido

Seguridad de datos de Amazon EBS

Los volúmenes de Amazon EBS se presentan como dispositivos de bloques sin formatear y sin procesar. Estos dispositivos son dispositivos lógicos que se crean en la infraestructura de EBS, y el servicio Amazon EBS garantiza que los dispositivos estén vacíos de forma lógica (es decir, los bloques sin procesar se establecen en cero o contienen datos criptográficamente pseudoaleatorios) antes de cualquier uso o reutilización por parte de un cliente.

Si tiene procedimientos que requieren que todos los datos se borren mediante un método específico, ya sea después o antes de su uso (o ambos), como los que se detallan en DoD 5220.22-M (National Industrial Security Program Operating Manual) o NIST 800-88 (Guidelines for Media Sanitization), puede hacerlo en Amazon EBS. Esa actividad de bloques se reflejará en los medios de almacenamiento subyacentes del servicio Amazon EBS.

Cifrado en reposo

Volúmenes de EBS

El cifrado de Amazon EBS es una solución de cifrado para volúmenes e instantáneas de EBS. Utiliza AWS KMS keys. Para obtener más información, consulte Cifrado de Amazon EBS en la Guía del usuario de Amazon EBS.

[Instancias de Windows] También puede utilizar permisos de Microsoft EFS y NTFS para el cifrado a nivel de carpeta y de archivo.

Volúmenes de almacén de instancias

Los datos incluidos en los volúmenes de almacén de instancias de NVMe se cifran con un cifrado XTS-AES-256 en un módulo de hardware de la instancia. Las claves utilizadas para cifrar los datos escritos en dispositivos de almacenamiento NVMe conectados localmente son por cliente y por volumen. Las claves las genera el módulo de hardware, al que no puede acceder el personal de AWS, y residen dentro de este. Las claves de cifrado se destruyen cuando se detiene o termina la instancia y no se pueden recuperar. No puede deshabilitar este cifrado ni tampoco proporcionar su propia clave de cifrado.

Los datos incluidos en los volúmenes de almacén de instancias de HDD en las instancias H1, D3 y D3en están cifrados con XTS-AES-256 y claves de un solo uso.

Cuando una instancia se detiene, se termina o se pone en hibernación, se restablecen todos los bloques de almacenamiento del volumen de almacén de instancias. Por lo tanto, no se puede obtener acceso a los datos a través del almacén de instancias de otra instancia.

Memoria

El cifrado de memoria se encuentra habilitado en las siguientes instancias:

- Instancias con procesadores AWS Graviton. AWS Graviton2, AWS Graviton3 y AWS Graviton3E admiten el cifrado de memoria siempre activo. Las claves de cifrado se generan de forma segura dentro del sistema host, no salen del sistema host y se destruyen al reiniciar o apagar el host. Para obtener más información, consulte Procesadores AWS Graviton.
- Instancias con procesadores escalables Intel Xeon de tercera generación (Ice Lake), como las instancias M6i, y procesadores escalables Intel Xeon de cuarta generación (Sapphire Rapids), como las instancias M7i. Estos procesadores admiten el cifrado de memoria siempre activo mediante Intel Total Memory Encryption (TME).
- Instancias con procesadores AMD EPYC de tercera generación (Milan), como las instancias M6a, y procesadores AMD EPYC de cuarta generación (Genoa), como las instancias M7a. Estos procesadores admiten el cifrado de memoria siempre activo mediante el cifrado seguro de

memoria (SME) de AMD. Las instancias con procesadores AMD EPYC de tercera generación (Milan) también son compatibles con la virtualización cifrada segura y la paginación anidada segura (SEV-SNP) de AMD.

Cifrado en tránsito

Cifrado en la capa física

Todos los datos que fluyen en las regiones de AWS a través de la red global de AWS se cifran automáticamente en la capa física antes de salir de las instalaciones seguras de AWS. Todo el tráfico entre las zonas de disponibiliad está cifrado. Las capas adicionales de cifrado, incluidas las que aparecen en esta sección, pueden proporcionar una protección adicional.

Cifrado proporcionado por la interconexión de Amazon VPC y la interconexión entre regiones de puerta de enlace de tránsito.

Todo el tráfico entre regiones que utiliza la interconexión de Amazon VPC y de puerta de enlace de tránsito se cifra de forma masiva automáticamente cuando sale de una región. De manera automática, se proporciona una capa adicional de cifrado en la capa física para todo el tráfico antes de dejar las instalaciones seguras de AWS, como se indicó anteriormente en esta sección.

Cifrado entre instancias

AWS proporciona conectividad privada y segura entre instancias de EC2 de todo tipo. Además, en algunos tipos de instancia, se utilizan las capacidades de descarga del hardware Nitro System subyacente para cifrar de manera automática el tráfico en tránsito entre instancias. Este cifrado utiliza algoritmos de encriptación autenticada con datos asociados (AEAD), con cifrado de 256 bits. No hay impacto en el rendimiento de la red. Para admitir este cifrado adicional del tráfico en tránsito entre instancias, se deben cumplir los siguientes requisitos:

- Las instancias utilizan los siguientes tipos de instancias:
  - De uso general: M5dn, M5n, M5zn, M6a, M6i, M6id, M6idn, M6in, M7a, M7g, M7gd, M7i, M7i-flex
  - Optimizadas para la computación: C5a, C5ad, C5n, C6a, C6gn, C6i, C6id, C6in, C7a, C7g, C7gd, C7gn, C7i, C7i-flex
  - Optimizadas para la memoria: R5dn, R5n, R6a, R6i, R6idn, R6in, R6id, R7a, R7g, R7gd, R7i, R7iz, U-3tb1, U-6tb1, U-9tb1, U-12tb1, U-18tb1, U-24tb1, U7i-12tb, U7in-16tb, U7in-24tb, U7in-32tb, X2idn, X2iedn, X2iezn
  - Optimizadas para el almacenamiento: D3, D3en, I3en, I4g, I4i, Im4gn, Is4gen

  - De computación acelerada: DL1, DL2q, G4ad, G4dn, G5, G6, Gr6, Inf1, Inf2, P3dn, P4d, P4de, P5, Trn1, Trn1n, VT1
  - De computación de alto rendimiento: Hpc6a, Hpc6id, Hpc7a, Hpc7g
- Las instancias se encuentran en la misma región.
- Las instancias están en la misma VPC o VPC interconectadas, y el tráfico no pasa a través de un dispositivo o servicio de red virtual, como un equilibrador de carga o una puerta de enlace de tránsito.

De manera automática, se proporciona una capa adicional de cifrado en la capa física para todo el tráfico antes de dejar las instalaciones seguras de AWS, como se indicó anteriormente en esta sección.

Para ver los tipos de instancias que cifran el tráfico en tránsito entre instancias mediante la AWS CLI

Utilice el siguiente comando: describe-instance-types.

```
aws ec2 describe-instance-types \
    --filters Name=network-info.encryption-in-transit-supported,Values=true \
    --query "InstanceTypes[*].[InstanceType]" \
    --output text | sort
```

Cifrado hacia y desde AWS Outposts

Un puesto de Outposts crea conexiones de red especiales llamadas enlaces de servicio en su región de inicio de AWS y, opcionalmente, conectividad privada a una subred VPC que especifique. Todo el tráfico a través de esa conexión está completamente cifrado. Para obtener más información, consulte Conectividad mediante enlaces de servicio y Cifrado en tránsito en laGuía del usuario de AWS Outposts.

Cifrado de acceso remoto

Los protocolos SSH y RDP proporcionan canales de comunicaciones seguros para el acceso remoto a las instancias, ya sea de forma directa o mediante EC2 Instance Connect. El acceso remoto a las instancias mediante AWS Systems Manager Session Manager o Run Command está cifrado con TLS 1.2, y las solicitudes para crear una conexión se firman con SigV4 y autentican y autorizan con AWS Identity and Access Management.

Es su responsabilidad utilizar un protocolo de cifrado como Transport Layer Security (TLS) para cifrar la información confidencial en tránsito entre los clientes y sus instancias de Amazon EC2.

(Instancias de Windows) Asegúrese de permitir solo conexiones cifradas entre las instancias EC2 y los puntos de conexión de la API de AWS u otros servicios de red remota confidenciales. Puede aplicar esto mediante un grupo de seguridad saliente o reglas de Firewall de Windows.

Seguridad de la infraestructura de Amazon EC2

Como se trata de un servicio administrado, Amazon Elastic Compute Cloud está protegido por la seguridad de red global de AWS. Para obtener información sobre los servicios de seguridad de AWS y cómo AWSprotege la infraestructura, consulte Seguridad en la nube de AWS. Para diseñar su entorno de AWS con las prácticas recomendadas de seguridad de infraestructura, consulte Protección de la infraestructura en Portal de seguridad de AWS Well-Architected Framework.

Puede utilizar llamadas a la API publicadas en AWS para acceder a Amazon EC2 a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad de seguridad de IAM principal. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Para obtener más información, consulte Protección de la infraestructura en el Pilar de seguridad: AWS Well-Architected Framework.

Aislamiento de red

Una Virtual Private Cloud (VPC) es una red virtual en su propia área, aislada lógicamente en la nube de AWS. Utilice VPC separados para aislar la infraestructura por carga de trabajo o unidad organizativa.

Una subred es un rango de direcciones IP de una VPC. Al iniciar una instancia, la lanza a una subred en su VPC. Utilice subredes para aislar los niveles de la aplicación (por ejemplo, web, aplicación y base de datos) en una VPC individual. Utilice subredes privadas para las instancias si no se debe acceder a ellas directamente desde Internet.

Para llamar a la API de Amazon EC2 desde la VPC mediante direcciones IP privadas, use AWS PrivateLink. Para obtener más información, consulte Acceso a Amazon EC2 mediante un punto de conexión de VPC de interfaz..

Aislamiento en hosts físicos

Las diferentes instancias de EC2 en un mismo host físico se aíslan unas de otras como si estuvieran en hosts físicos distintos. El hipervisor aísla la CPU y la memoria, y a las instancias se les proporcionan discos virtualizados en lugar de acceso a los dispositivos del disco sin procesar.

Al detener o finalizar una instancia, el hipervisor limpia la memoria que tiene asignada (la establece en cero) antes de asignarla a una instancia nueva. Además, se restablece cada bloque de almacenamiento. Esto garantiza que los datos no se expongan de forma involuntaria a otra instancia.

Las direcciones MAC de la red se asignan de forma dinámica a las instancias mediante la infraestructura de red de AWS. Las direcciones IP o bien las asigna la infraestructura de red de AWS de forma dinámica a las instancias o bien las asigna un administrador de EC2 mediante solicitudes API autenticadas. La red de AWS permite que las instancias envíen tráfico únicamente desde las direcciones MAC e IP que tienen asignadas. De lo contrario, el tráfico se corta.

De forma predeterminada, una instancia no puede recibir tráfico que no esté dirigido específicamente a ella. Si tiene que ejecutar servicios de traducción de direcciones de red (NAT), de direccionamiento o de firewall en la instancia, puede desactivar la comprobación de origen o destino para la interfaz de red.

Control del tráfico de red

Tenga en cuenta las siguientes opciones para controlar el tráfico de red a las instancias de EC2:

- Limite el acceso a las instancias mediante el uso de grupos de seguridad. Configure reglas que permitan el tráfico de red mínimo requerido. Por ejemplo, puede permitir el tráfico únicamente desde rangos de direcciones para su red corporativa o solo para protocolos específicos, como HTTPS. En el caso de las instancias de Windows, permita el tráfico de administración de Windows y conexiones salientes mínimas.
- Aproveche los grupos de seguridad como mecanismo principal para controlar el acceso de la red a las instancias Amazon EC2. Cuando sea necesario, utilice las ACL de red con moderación para proporcionar un control de red sin estado y amplio. Los grupos de seguridad son más versátiles que las ACL de red debido a su capacidad de realizar un filtrado de paquetes con estado y crear reglas que hagan referencia a otros grupos de seguridad. Sin embargo, las ACL de red

pueden ser eficaces como control secundario para denegar un subconjunto específico de tráfico o proporcionar medidas de protección de subred de alto nivel. Además, dado que las ACL de red se aplican a toda una subred, se pueden utilizar como defensa en profundidad en caso de que una instancia se lance involuntariamente sin un grupo de seguridad correcto.

- [Instancias de Windows] Administre de forma centralizada la configuración de Firewall de Windows con objetos de políticas de grupo (GPO) para mejorar aún más los controles de red. Los clientes suelen utilizar el Firewall de Windows para obtener una mayor visibilidad del tráfico de red y complementar los filtros de grupos de seguridad, creando reglas avanzadas para impedir que aplicaciones específicas accedan a la red o para filtrar el tráfico de un subconjunto de direcciones IP. Por ejemplo, el Firewall de Windows puede limitar el acceso a la dirección IP del servicio de metadatos de EC2 a usuarios o aplicaciones específicos. Como alternativa, un servicio público podría utilizar grupos de seguridad para restringir el tráfico a puertos específicos y el Firewall de Windows a fin de mantener una lista de direcciones IP bloqueadas explícitamente.
- Utilice subredes privadas para las instancias si no se debe acceder a ellas directamente desde Internet. Utilice un host bastión o puerta de enlace de NAT para acceder a Internet desde una instancia en una subred privada.
- [Instancias de Windows] Use protocolos de administración seguros como la encapsulación RDP sobre SSL/TLS. El inicio rápido de la puerta de enlace de escritorio remoto ofrece prácticas recomendadas para implementar la puerta de enlace de escritorio remoto, incluida la configuración de RDP para usar SSL/TLS.
- [Instancias de Windows] Utilice Active Directory o AWS Directory Service para controlar y supervisar de forma estricta y centralizada el acceso interactivo de usuarios y grupos a instancias de Windows y evitar los permisos de usuarios locales. Evite también el uso de administradores de dominio y, en su lugar, cree cuentas basadas en roles más detalladas y específicas de la aplicación. Just Enough Administration (JEA) permite administrar los cambios en las instancias de Windows sin acceso interactivo o de administrador. Además, JEA permite a las organizaciones bloquear el acceso administrativo al subconjunto de comandos de Windows PowerShell necesarios para la administración de instancias. Para obtener información adicional, consulte la sección “Administración del acceso a Amazon EC2 de nivel de sistema operativo” en el documento técnico Prácticas recomendadas de seguridad de AWS.
- [Instancias de Windows] Los administradores de sistemas deben usar cuentas de Windows con acceso limitado para realizar actividades diarias y elevar el acceso solo cuando sea necesario para realizar cambios de configuración específicos. Además, acceda directamente a las instancias de Windows solo cuando sea absolutamente necesario. En su lugar, aproveche los sistemas de administración de la configuración central como EC2 Run Command, Systems Center

Configuration Manager (SCCM), Windows PowerShell DSC o Amazon EC2 Systems Manager (SSM) para introducir cambios en los servidores de Windows.

- Configure tablas de enrutamiento de subred de Amazon VPC con las rutas de red mínimas requeridas. Por ejemplo, coloque solo las instancias de Amazon EC2 que requieran acceso directo a Internet en subredes con rutas a una puerta de enlace de Internet y coloque solo las instancias de Amazon EC2 que necesiten acceso directo a redes internas en subredes con rutas a una puerta de enlace privada virtual.
- Considere la posibilidad de utilizar grupos de seguridad adicionales o interfaces de red para controlar y auditar el tráfico de administración de instancias de Amazon EC2 con independencia del tráfico normal de aplicaciones. Este enfoque permite a los clientes implementar políticas especiales de IAM para el control de cambios, lo que facilita la auditoría de los cambios en reglas de grupos de seguridad o en los scripts automatizados de verificación de reglas. El uso de múltiples interfaces de red también ofrece opciones adicionales para controlar el tráfico de red, incluida la capacidad de crear políticas de direccionamiento basadas en el host o aprovechar diferentes reglas de direccionamiento de la subred de la VPC basadas en una subred asignada de la interfaz de red.
- Utilice AWS Virtual Private Network o AWS Direct Connect para establecer conexiones privadas desde sus redes remotas a sus VPC. Para obtener más información, consulte la sección sobre opciones de conectividad entre la red y Amazon VPC.
- Utilice registros de flujo de VPC para monitorear el tráfico que llegue a sus instancias.
- Utilice Protección contra malware de GuardDuty para identificar comportamientos sospechosos que indiquen la presencia de software malicioso en sus instancias y que puedan comprometer su carga de trabajo, reutilizar los recursos para usos malintencionados y obtener acceso no autorizado a sus datos.
- Utilice el Monitoreo de tiempo de ejecución GuardDuty para identificar las posibles amenazas a sus instancias y responder a ellas. Para obtener más información, consulte Cómo funciona el Monitoreo de tiempo de ejecución con las instancias de Amazon EC2.
- Utilice AWS Security Hub, el Analizador de accesibilidad o el Analizador de acceso a la red para comprobar si sus instancias acceden a la red de forma no intencionada.
- Utilice EC2 Instance Connect para conectarse a sus instancias desde Secure Shell (SSH) sin compartir ni administrar claves SSH.
- Utilice Session Manager de AWS Systems Manager para acceder a las instancias remotamente en lugar de abrir puertos SSH o RDP de entrada y administrar pares de claves.

- Utilice Run Command de AWS Systems Manager para automatizar las tareas administrativas comunes en lugar de conectarse a sus instancias.
- [Instancias de Windows] Muchos de los roles del sistema operativo Windows y las aplicaciones empresariales de Microsoft también proporcionan funcionalidad mejorada, como restricciones de rango de direcciones IP dentro de IIS, políticas de filtrado TCP/IP en Microsoft SQL Server y políticas de filtro de conexión en Microsoft Exchange. La funcionalidad de restricción de red dentro de la capa de aplicación puede proporcionar capas adicionales de defensa para los servidores de aplicaciones empresariales críticos.

Amazon VPC admite controles de seguridad de red adicionales, como puertas de enlace, servidores proxy y opciones de monitoreo de red. Para obtener más información, consulte Control del tráfico de red en la Guía del usuario de Amazon VPC.

Resiliencia en Amazon EC2

La infraestructura global de AWS está conformada por regiones y zonas de disponibilidad de AWS. Las regiones proporcionan varias zonas de disponibilidad físicamente independientes y aisladas que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja latencia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de centros de datos únicos o múltiples.

Si necesita replicar datos o aplicaciones sobre grandes distancias geográficas, utilice AWS Local Zones. Una zona local de AWS es una extensión de una región de AWS cercana geográficamente a los usuarios. Las Local Zones tienen sus propias conexiones a Internet y admiten AWS Direct Connect. Al igual que en el caso de todas las regiones de AWS, las AWS Local Zones se encuentran completamente aisladas de las demás zonas de AWS.

Si necesita replicar sus datos o aplicaciones en una zona local de AWS, AWS recomienda utilizar una de las siguientes zonas como zona de conmutación por error:

- Otra zona local
- Zona de disponibilidad en la región que no es la zona principal. Puede utilizar el comando describe-availability-zones para ver la zona principal.

Para obtener más información sobre zonas de disponibilidad y las regiones de AWS, consulte Infraestructura global de AWS.

Además de la infraestructura global de AWS, Amazon EC2 ofrece las siguientes características que respaldan la resiliencia de datos:

- Copia de las AMI entre regiones
- Copia de las instantáneas de EBS en las regiones
- Automatización de las AMI respaldadas por EBS con Amazon Data Lifecycle Manager
- Automatización de las instantáneas de EBS con Amazon Data Lifecycle Manager
- Mantenimiento del buen estado y la disponibilidad de su flota con Amazon EC2 Auto Scaling
- Puede distribuir el tráfico entrante entre las distintas instancias en una única o en varias zonas de disponibilidad con Elastic Load Balancing.

Validación de la conformidad en Amazon EC2

Para saber si un Servicio de AWS está incluido en el ámbito de programas de conformidad específicos, consulte Servicios de AWS en el ámbito del programa de conformidad y elija el programa de conformidad que le interese. Para obtener información general, consulte Programas de conformidad de AWS.

Puede descargar los informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact.

Su responsabilidad de conformidad al utilizar Servicios de AWS se determina en función de la sensibilidad de los datos, los objetivos de cumplimiento de su empresa y la legislación y los reglamentos correspondientes. AWS proporciona los siguientes recursos para ayudar con la conformidad:

- Guías de inicio rápido de seguridad y conformidad: estas guías de implementación tratan consideraciones sobre arquitectura y ofrecen pasos para implementar los entornos de referencia centrados en la seguridad y la conformidad en AWS.
- Architecting for HIPAA Security and Compliance on Amazon Web Services (Arquitectura para la seguridad y el cumplimiento de la HIPAA en Amazon Web Services): en este documento técnico, se describe cómo las empresas pueden utilizar AWS para crear aplicaciones aptas para HIPAA.

> **Note**
>
> No todos los Servicios de AWS son aptos para HIPAA. Para más información, consulte la Referencia de servicios compatibles con HIPAA.

- Recursos de conformidad de AWS: este conjunto de manuales y guías podría aplicarse a su sector y ubicación.
- Guías de cumplimiento para clientes de AWS: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad de los Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés), el Consejo de Estándares de Seguridad de la Industria de Tarjetas de Pago (PCI, por sus siglas en inglés) y la Organización Internacional de Normalización (ISO, por sus siglas en inglés)).
- Evaluación de recursos con reglas en la Guía para desarrolladores de AWS Config: el servicio AWS Config evalúa en qué medida las configuraciones de sus recursos cumplen las prácticas internas, las directrices del sector y las normativas.
- AWS Security Hub: este Servicio de AWS proporciona una visión completa de su estado de seguridad en AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.
- Amazon GuardDuty: este Servicio de AWS detecta posibles amenazas para sus Cuentas de AWS, cargas de trabajo, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a satisfacer varios requisitos de conformidad, como PCI DSS, cumpliendo los requisitos de detección de intrusos que exigen determinados marcos de conformidad.
- AWS Audit Manager: este servicio de Servicio de AWS le ayuda a auditar continuamente el uso de AWS con el fin de simplificar la forma en que administra el riesgo y la conformidad con las normativas y los estándares del sector.

Identity and Access Management para Amazon EC2

Las credenciales de seguridad sirven para identificarlo ante los servicios de AWS y le otorgan uso ilimitado de sus recursos de AWS, como, por ejemplo, los recursos de Amazon EC2. Puede utilizar características de Amazon EC2 y AWS Identity and Access Management (IAM) para permitir que

otros usuarios, servicios y aplicaciones utilicen sus recursos de Amazon EC2 sin necesidad de compartir sus credenciales de seguridad. Puede utilizar IAM para controlar la forma en que otros usuarios usan los recursos de su cuenta de AWS y puede utilizar los grupos de seguridad para controlar el acceso a sus instancias de Amazon EC2. Puede optar por permitir un uso completo o limitado de sus recursos de Amazon EC2.

Para conocer las prácticas recomendadas destinadas a asegurar los recursos de AWS que utilizan IAM, consulte Prácticas recomendadas de seguridad en IAM.

Contenido

Acceso de red a su instancia

Un grupo de seguridad funciona como un firewall que controla el tráfico que puede llegar a una o varias instancias. Cuando lanza una instancia, la asigna a uno o varios grupos de seguridad. Añade reglas a cada grupo de seguridad que controla el tráfico de la instancia. Puede modificar las reglas de un grupo de seguridad en cualquier momento; las nuevas reglas se aplican automáticamente a todas las instancias a las que el grupo de seguridad esté asignado.

Para obtener más información, consulte Reglas del grupo de seguridad.

Atributos de los permisos de Amazon EC2

Su organización puede tener varias cuentas de AWS. Amazon EC2 le permite especificar cuentas de AWS adicionales que pueden utilizar sus imágenes de máquina de Amazon (AMI) e instantáneas de Amazon EBS. Estos permisos funcionan únicamente en el nivel de cuenta de AWS; no puede restringir los permisos a usuarios concretos de la cuenta de AWS especificada. Todos los usuarios de la cuenta de AWS que ha especificado pueden utilizar la AMI o la instantánea.

Cada AMI tiene un atributo `LaunchPermission` que controla las cuentas de AWS que pueden obtener acceso a ella. Para obtener más información, consulte Convertir una AMI en pública.

Cada instantánea de Amazon EBS tiene un atributo `createVolumePermission` que controla qué cuentas de AWS pueden utilizar la instantánea. Para obtener más información, consulte Compartir una instantánea de Amazon EBS en la Guía del usuario de Amazon EBS.

IAM y Amazon EC2

IAM le permite hacer lo siguiente:

- Crear usuarios y grupos en su Cuenta de AWS
- Asignar credenciales de seguridad únicas a cada usuario en su Cuenta de AWS
- Controlar los permisos de cada usuario para realizar tareas mediante recursos de AWS
- Permitir a los usuarios de otra Cuenta de AWS compartir sus recursos de AWS
- Crear roles para su Cuenta de AWS y definir los usuarios o servicios que pueden asumirlos
- Usar identidades existentes para que su compañía conceda permisos para realizar tareas mediante recursos de AWS

Si utiliza IAM con Amazon EC2, podrá controlar si los usuarios de su organización pueden realizar una tarea mediante acciones específicas de la API de Amazon EC2 y si pueden utilizar recursos específicos de AWS.

Este tema le ayuda a responder las preguntas siguientes:

- ¿Cómo puedo crear grupos y usuarios en IAM?
- ¿Cómo creo una política?
- ¿Qué políticas de IAM necesito para llevar a cabo tareas en Amazon EC2?
- ¿Cómo concedo permisos para realizar acciones en Amazon EC2?
- ¿Cómo concedo permisos para realizar acciones en recursos específicos de Amazon EC2?

Creación de usuarios, grupos y roles

Puede crear usuarios y grupos para su Cuenta de AWS y, a continuación, asignarles los permisos que necesiten. Como práctica recomendada, los usuarios deben adquirir los permisos al asumir roles de IAM.

Un rol de IAM es una identidad de IAM que puede crear en su cuenta y que tiene permisos específicos. Un rol de IAM es similar a un usuario de IAM en que se trata de una identidad de AWS

con políticas de permisos que determinan lo que la identidad puede hacer y lo que no en AWS. No obstante, en lugar de asociarse exclusivamente a una persona, la intención es que cualquier usuario pueda asumir un rol que necesite. Además, un rol no tiene asociadas credenciales a largo plazo estándar, como una contraseña o claves de acceso. En su lugar, cuando se asume un rol, este proporciona credenciales de seguridad temporales para la sesión de rol. Para obtener más información sobre cómo crear roles de IAM y conceder permisos con ellos, consulte the section called “IAM roles”.

Temas relacionados de

Para obtener más información sobre IAM, consulte lo siguiente:

- Políticas de IAM para Amazon EC2
- Roles de IAM para Amazon EC2
- AWS Identity and Access Management (IAM)
- Guía del usuario de IAM

Políticas de IAM para Amazon EC2

De forma predeterminada, los usuarios no tienen permiso para crear ni modificar recursos de Amazon EC2, ni para realizar tareas con la API de Amazon EC2, la consola de Amazon EC2 o la CLI. Para permitir a los usuarios crear o modificar recursos y realizar tareas, debe crear políticas de IAM que concedan a los usuarios permisos para utilizar los recursos y las acciones de la API que necesitarán y, a continuación, asociar dichas políticas a los usuarios, grupos o roles de IAM que requieran dichos permisos.

Cuando asocia una política a un usuario, grupo de usuarios o rol, les otorga o deniega el permiso para realizar las tareas especificadas en los recursos indicados. Para obtener más información general sobre las políticas de IAM, consulte Políticas y permisos en IAM en la Guía del usuario de IAM. Para obtener más información sobre cómo crear y administrar políticas de IAM personalizadas, consulte Administración de políticas de IAM.

Introducción

Una política de IAM debe conceder o denegar permisos para usar una o varias acciones de Amazon EC2. Asimismo, debe especificar los recursos que se pueden utilizar con la acción: pueden ser todos los recursos o, en algunos casos, recursos específicos. La política también puede incluir condiciones que se aplican al recurso.

Amazon EC2 admite parcialmente permisos de nivel de recurso. Esto significa que en algunas acciones de la API de EC2 no puede especificar qué recurso puede utilizar un usuario para la acción en cuestión. En lugar de ello, tiene que permitir a los usuarios trabajar con todos los recursos para dicha acción.

Tarea	Tema
Comprender la estructura básica de una política	Sintaxis de la política
Definir acciones en una política	Acciones de Amazon EC2
Definir recursos específicos en una política	Nombres de recursos de Amazon (ARN) para Amazon EC2
Aplicar condiciones para usar los recursos	Claves de condición de Amazon EC2
Trabajar con permisos de nivel de recursos disponibles para Amazon EC2	Acciones, recursos y claves de condiciones para Amazon EC2
Probar su política	Comprobar que los usuarios tienen los permisos necesarios
Generar una política de IAM	Generar políticas basadas en la actividad de acceso
Políticas de ejemplo para una CLI o SDK	Políticas de ejemplo para trabajar con la AWS CLI o un SDK de AWS
Políticas de ejemplo para la consola de Amazon EC2	Políticas de ejemplo para trabajar en la consola de Amazon EC2

Concesión de permisos a usuarios, grupos y roles

A continuación, se muestran ejemplos de algunas políticas administradas por AWS que están disponibles para utilizarse si satisfacen sus necesidades:

- `PowerUserAccess`
- `ReadOnlyAccess`

- `AmazonEC2FullAccess`
- `AmazonEC2ReadOnlyAccess`

Para obtener más información, consulte the section called “Políticas administradas de AWS”.

Para dar acceso, agregue permisos a los usuarios, grupos o roles:

- Usuarios y grupos en AWS IAM Identity Center:

  Cree un conjunto de permisos. Siga las instrucciones de Creación de un conjunto de permisos en la Guía del usuario de AWS IAM Identity Center.
- Usuarios administrados en IAM a través de un proveedor de identidades:

  Cree un rol para la federación de identidades. Siga las instrucciones descritas en Creación de un rol para un proveedor de identidad de terceros (federación) en la Guía del usuario de IAM.
- Usuarios de IAM:
  - Cree un rol que el usuario pueda aceptar. Siga las instrucciones descritas en Creación de un rol para un usuario de IAM en la Guía del usuario de IAM.
  - (No recomendado) Adjunte una política directamente a un usuario o añada un usuario a un grupo de usuarios. Siga las instrucciones descritas en Adición de permisos a un usuario (consola) de la Guía del usuario de IAM.

Estructura de la política

En los siguientes temas se explica la estructura de una política de IAM.

Contenido

Sintaxis de la política

Una política de IAM es un documento JSON que contiene una o varias instrucciones. Cada instrucción tiene la estructura siguiente.

```
{
  "Statement":[{
    "Effect":"effect",
    "Action":"action",
    "Resource":"arn",
    "Condition":{
      "condition":{
        "key":"value"
        }
      }
    }
  ]
}
```

Una instrucción está compuesta por varios elementos:

- Effect: el valor de effect puede ser `Allow` o `Deny`. De forma predeterminada, los usuarios no tienen permiso para utilizar los recursos y las acciones de la API, por lo que se deniegan todas las solicitudes. Si se concede un permiso explícito se anula el valor predeterminado. Una denegación explícita invalida cualquier permiso concedido.
- Action: el valor de action es la acción de la API para la que concede o deniega permisos. Para obtener más información de cómo especificar el valor de action, consulte Acciones de Amazon EC2.
- Resource: el recurso al que afecta la acción. Algunas acciones de la API de Amazon EC2 permiten incluir en la política recursos específicos que la acción puede crear o modificar. Especifique un recurso con un nombre de recurso de Amazon (ARN) o utilizando el carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos. Para obtener más información, consulte Permisos de nivel de recurso admitidos para las acciones de la API de Amazon EC2.
- Condition: las condiciones son opcionales. Se pueden usar para controlar cuándo está en vigor la política. Para obtener más información sobre cómo especificar condiciones para Amazon EC2, consulte Claves de condición de Amazon EC2.

Para obtener más información sobre los requisitos de la política, consulte la Referencia de la política JSON de IAM en la Guía del usuario de IAM. Para obtener ejemplos de instrucciones de política de

IAM para Amazon EC2, consulte Políticas de ejemplo para trabajar con la AWS CLI o un SDK de AWS.

Acciones de Amazon EC2

En una instrucción de política de IAM, puede especificar cualquier acción de API de cualquier servicio que sea compatible con IAM. Para Amazon EC2, use el prefijo siguiente con el nombre de la acción de API: `ec2:`. Por ejemplo: `ec2:RunInstances` y `ec2:CreateImage`.

Para especificar varias acciones en una única instrucción, sepárelas con comas del siguiente modo:

```
"Action": ["ec2:action1", "ec2:action2"]
```

También puede utilizar caracteres comodín para especificar varias acciones. Por ejemplo, puede especificar todas las acciones cuyo nombre comience por la palabra "Describe" del siguiente modo:

```
"Action": "ec2:Describe*"
```

> **Note**
>
> Actualmente, las acciones de la API de Amazon EC2 Describe* no admiten permisos de nivel de recurso. Para obtener más información sobre los permisos de nivel de recursos para Amazon EC2, consulte Políticas de IAM para Amazon EC2.

Para especificar todas las acciones de API de Amazon EC2, use el carácter comodín * del siguiente modo:

```
"Action": "ec2:*"
```

Para ver una lista de las acciones de Amazon EC2, consulte Acciones definidas por Amazon EC2 en la referencia de autorizaciones de servicio.

Permisos de nivel de recurso admitidos para las acciones de la API de Amazon EC2

Los permisos de nivel de recursos hacen referencia a la capacidad de especificar en qué recursos los usuarios tienen permitido realizar acciones. Amazon EC2 admite parcialmente los permisos de nivel de recursos. Esto significa que, en algunas acciones de Amazon EC2, puede determinar cuándo se permite utilizarlas a los usuarios en función de si se cumplen una serie de condiciones o de los recursos concretos que pueden utilizar los usuarios. Por ejemplo, puede otorgar permisos a

los usuarios para iniciar instancias, pero solo de un tipo específico, y únicamente utilizando una AMI específica.

Para especificar un recurso en la instrucción de política de IAM, se utiliza el nombre de recurso de Amazon (ARN). Para obtener más información sobre cómo especificar el valor de ARN, consulte Nombres de recursos de Amazon (ARN) para Amazon EC2. Si una acción de API no admite ARN individuales, debe utilizar un comodín (*) para especificar que la acción puede afectar a todos los recursos.

Para ver tablas que identifican qué acciones de la API de Amazon EC2 admiten permisos de nivel de recursos, así como los ARN y las claves de condición que puede usar en una política, consulte Acciones, recursos y claves de condición para Amazon EC2.

Tenga en cuenta que puede aplicar permisos de nivel de recurso basados en etiquetas en las políticas de IAM que utiliza para acciones de la API de Amazon EC2. Esto le ofrece un mejor control sobre los recursos que un usuario puede crear, modificar o utilizar. Para obtener más información, consulte Conceder permisos para etiquetar recursos durante la creación.

Nombres de recursos de Amazon (ARN) para Amazon EC2

Cada instrucción de política de IAM se aplica a los recursos especificados utilizando sus ARN.

Un ARN tiene la siguiente sintaxis general:

```
arn:aws:[service]:[region]:[account-id]:resourceType/resourcePath
```

service

El servicio (por ejemplo, `ec2`).

region

La región para el recurso (por ejemplo `us-east-1`).

account-id

El ID de cuenta de AWS, sin guiones (por ejemplo, `123456789012`).

resourceType

El tipo de recurso (por ejemplo, `instance`).

resourcePath

Una ruta que identifica al recurso. Puede utilizar carácter comodín * en las rutas.

Por ejemplo, puede indicar una instancia específica (`i-1234567890abcdef0`) en la instrucción usando su ARN de este modo.

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0"
```

También puede especificar todas las instancias que pertenecen a una cuenta específica mediante el carácter comodín * del modo siguiente.

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/*"
```

También puede especificar todos los recursos de Amazon EC2 que pertenecen a una cuenta específica mediante el carácter comodín * del modo siguiente.

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:*"
```

Para especificar todos los recursos o cuando una acción de API no admita ARN, utilice el carácter comodín * en el elemento `Resource` de la siguiente manera.

```
"Resource": "*"
```

En muchas acciones de la API de Amazon EC2 se utilizan varios recursos. Por ejemplo, `AttachVolume` asocia un volumen de Amazon EBS a una instancia, por lo que un usuario debe tener permisos para utilizar el volumen y la instancia. Para especificar varios recursos en una única instrucción, separe sus ARN con comas, tal y como se indica a continuación.

```
"Resource": ["arn1", "arn2"]
```

Para obtener una lista de ARN de recursos de Amazon EC2, consulte Tipos de recursos definidos por Amazon EC2.

Claves de condición de Amazon EC2

En la instrucción de una política, tiene la opción de especificar las condiciones que controlan cuando está en vigor. Cada condición contiene uno o varios pares clave-valor. Las claves de condición no distinguen entre mayúsculas y minúsculas. Hemos definido claves de condición globales de AWS y también claves de condición específicas de los servicios.

Para obtener una lista de las claves de condición específicas del servicio para Amazon EC2, consulte Claves de condición para Amazon EC2. Amazon EC2 también implementa las claves de condición

globales de AWS. Para obtener más información, consulte Información disponible en todas las solicitudes en la Guía del usuario de IAM.

Para utilizar una clave de condición en la política de IAM, utilice la instrucción `Condition`. Por ejemplo, la política siguiente concede a los usuarios permiso para agregar y eliminar reglas de entrada y salida para cualquier grupo de seguridad. Utiliza la clave de condición `ec2:Vpc` para especificar que estas acciones solo se pueden realizar en grupos de seguridad de una VPC específica.

```
{
"Version": "2012-10-17",
  "Statement":[{
    "Effect":"Allow",
    "Action": [
       "ec2:AuthorizeSecurityGroupIngress",
       "ec2:AuthorizeSecurityGroupEgress",
       "ec2:RevokeSecurityGroupIngress",
       "ec2:RevokeSecurityGroupEgress"],
     "Resource": "arn:aws:ec2:region:account:security-group/*",
      "Condition": {
        "StringEquals": {
          "ec2:Vpc": "arn:aws:ec2:region:account:vpc/vpc-11223344556677889"
        }
      }
    }
  ]
}
```

Si especifica varias condiciones o varias claves en una condición, las evaluamos con una operación lógica AND. Si especifica una condición con varios valores para una clave, evaluamos la condición con una operación lógica OR. Para conceder los permisos, es necesario que se cumplan todas las condiciones.

También puede utilizar comodines al especificar las condiciones. Para obtener más información, consulte Elementos de la política de IAM: Variables y etiquetas en la Guía del usuario de IAM.

> **Important**
>
> Muchas claves de condición son específicas de un recurso y algunas acciones de API utilizan varios recursos. Si escribe una política con una clave de condición, use el elemento `Resource` de la instrucción para especificar el recurso en el que se aplica la clave de

condición. Si no lo hace, la política puede impedir que los usuarios ejecuten la acción, ya que la comprobación de la condición dará un error en el caso de los recursos en los que la clave de la condición no se aplica. Si no quiere especificar un recurso o si ha escrito el elemento `Action` de su política para que contenga varias acciones de API, debe utilizar el tipo de condición `...IfExists` para asegurarse de que no se tenga en cuenta la clave de condición en el caso de los recursos que no la utilicen. Para obtener más información, consulte ...IfExists Conditions en la Guía del usuario de IAM.

Todas las acciones de Amazon EC2 admiten las claves de condición `aws:RequestedRegion` y `ec2:Region`. Para obtener más información, consulte Ejemplo: Restringir el acceso a una región específica.

Clave de condición de **`ec2:SourceInstanceARN`**

La clave de condición `ec2:SourceInstanceARN` se puede utilizar para condiciones que especifiquen el ARN de la instancia desde la que se realiza una solicitud. Esta es una clave de condición global de AWS y no es específica de un servicio. Para ver ejemplos de políticas, consulte Amazon EC2: asociar o separar volúmenes de una instancia de EC2 y Ejemplo: Permitir que una instancia específica vea los recursos de otros servicios de AWS. La clave `ec2:SourceInstanceARN` no se puede usar como una variable para rellenar el ARN del elemento `Resource` en una instrucción.

Para obtener ejemplos de instrucciones de política de Amazon EC2, consulte Políticas de ejemplo para trabajar con la AWS CLI o un SDK de AWS.

Clave de condición de **`ec2:Attribute`**

La clave de condición `ec2:Attribute` se puede utilizar para condiciones que filtran el acceso por un atributo de un recurso. La clave de condición solo admite propiedades que son de un tipo de datos primitivo (como una cadena o un entero), u objetos AttributeValue complejos que tienen solo una propiedad Valor (como los objetos Descripción o ImdsSupport de la acción de la API ModifyImageAttribute).

Important

La clave de condición no se puede usar con objetos complejos que tengan varias propiedades, como el objeto LaunchPermission de la acción de la API ModifyImageAttribute.

Por ejemplo, la siguiente política utiliza la clave de condición `ec2:Attribute/Description` para filtrar el acceso por parte del objeto complejo Descripción de la acción ModifyImageAttribute de la API. La clave de condición solo permite solicitudes que modifican la descripción de una imagen `Production` o `Development`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:ModifyImageAttribute",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-*",
      "Condition": {
        "StringEquals": {
          "ec2:Attribute/Description": [
            "Production",
            "Development"
          ]
        }
      }
    }
  ]
}
```

El ejemplo siguiente de política utiliza la clave de condición `ec2:Attribute` para filtrar el acceso mediante la propiedad primitiva Atributo de la acción ModifyImageAttribute de la API. La clave de condición deniega todas las solicitudes que intentan modificar la descripción de una imagen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "ec2:ModifyImageAttribute",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-*",
      "Condition": {
        "StringEquals": {
          "ec2:Attribute": "Description"
        }
      }
    }
  ]
```

```
}
```

Claves de condición de **ec2:ResourceID**

Cuando utilice las siguientes claves de condición `ec2:ResourceID` con las acciones de API especificadas, el valor de la clave de condición se utiliza para especificar el recurso resultante que se crea mediante la acción de la API. Las claves de condición `ec2:ResourceID` no se pueden usar para especificar un recurso fuente que se especifica en la solicitud de la API.
Si usa una de las siguientes claves de condición `ec2:ResourceID` con una API específica, entonces siempre debe especificar el comodín (*). Si especifica un valor diferente, la condición siempre se resuelve como * durante el tiempo de ejecución. Por ejemplo, para usar la clave de condición `ec2:ImageId` con la API CopyImage, luego debe especificar la clave de condición de la siguiente manera:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CopyImage",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-*",
      "Condition": {
        "StringEquals": {
          ec2:ImageID": "*"
        }
      }
    }
  ]
}
```

Clave de condición	Acción de la API			
`ec2:Dhcp0ptionsID`	• CreateDhcpOptions			
`ec2:ImageID`	•			

Clave de condición	Acción de la API			
	CopyImage • CreateImage • ImportImage • RegisterImage			
ec2:InstanceID	• RunInstances • ImportInstance			
ec2:InternetGatewayID	• CreateInternetGateway			
ec2:NetworkAclID	• CreateNetworkAcl			
ec2:NetworkInterfaceID	• CreateNetworkInterface			
ec2:PlacementGroupName	• CreatePlacementGroup			

Clave de condición	Acción de la API			
`ec2:RouteTableID`	• CreateRouteTable			
`ec2:SecurityGroupID`	• CreateSecurityGroup			
`ec2:SnapshotID`	• CopySnapshot • CreateSnapshot • CreateSnapshots • ImportSnapshots			
`ec2:SubnetID`	• CreateSubnet			
`ec2:VolumeID`	• CreateVolume • ImportVolume			
`ec2:VpcID`	• CreateVpc			

Clave de condición	Acción de la API			
`ec2:VpcPeeringConnectionID`	• CreateVpcPeeringConnection			

Recomendamos que evite usar las claves de condición `ec2:`*`Resource`*`ID` con estas acciones de API. En cambio, si necesita filtrar el acceso en función de identificadores de recursos específicos, recomendamos que lo haga mediante el elemento de política `Resource`, de la siguiente manera:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CopyImage",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-01234567890abcdef"
    }
  ]
}
```

Comprobar que los usuarios tienen los permisos necesarios

Una vez creada la política de IAM, le recomendamos que compruebe si concede permisos a los usuarios para utilizar las acciones de la API concretas y los recursos necesarios antes de pasar la política a producción.

En primer lugar, cree un usuario para realizar pruebas y, a continuación, asocie la política de IAM que creó al usuario de prueba. A continuación, realice una solicitud como usuario de prueba.

Si la acción de Amazon EC2 que va a probar crea o modifica un recurso, debería efectuar la solicitud mediante el parámetro `DryRun` (o ejecutar el comando de la AWS CLI con la opción `--dry-run`). En este caso, la llamada completa la comprobación de autorización, pero no la operación. Por ejemplo, puede comprobar si el usuario puede finalizar una instancia determinada sin finalizarla en realidad. Si el usuario de prueba tiene los permisos necesarios, la solicitud devolverá `DryRunOperation`; de lo contrario, devolverá `UnauthorizedOperation`.

Si la política no concede los permisos previstos al usuario o es demasiado permisiva, puede ajustarla según sea necesario y repetir las pruebas hasta obtener el resultado deseado.

> **Important**
>
> Puede que los cambios en la política tarden varios minutos en propagarse y surtir efecto. Por lo tanto, le recomendamos que espere cinco minutos antes de probar las actualizaciones de la misma.

Si se produce un error en la comprobación de autorización, la solicitud devuelve un mensaje codificado con información de diagnóstico. Puede descodificar el mensaje usando la acción `DecodeAuthorizationMessage`. Para obtener más información, consulte DecodeAuthorizationMessage en la Referencia de la API de AWS Security Token Service y decode-authorization-message en la Referencia de comandos de la AWS CLI.

Conceder permisos para etiquetar recursos durante la creación

Algunas acciones de la API de Amazon EC2 de creación de recursos le permiten especificar etiquetas al crear el recurso. Puede utilizar etiquetas de recursos para implementar el control basado en atributos (ABAC). Para obtener más información, consulte Etiquetar los recursos y Control del acceso a recursos de EC2 mediante etiquetas de recursos.

Para permitir que los usuarios etiqueten los recursos durante su creación, es preciso que tengan permisos para utilizar la acción que crea el recurso (por ejemplo, `ec2:RunInstances` o `ec2:CreateVolume`). Si se especifican etiquetas en la acción de creación de recursos, Amazon realiza una autorización adicional en la acción `ec2:CreateTags` para verificar que los usuarios tengan permisos para crear etiquetas. Por lo tanto, los usuarios también deben tener permisos explícitos para usar la acción `ec2:CreateTags`.

En la definición de la política de IAM de la acción `ec2:CreateTags`, utilice el elemento `Condition` con la clave de condición `ec2:CreateAction` para otorgar permisos de etiquetado a la acción que crea el recurso.

En el ejemplo siguiente se muestra una política que permite a los usuarios iniciar instancias y aplicar cualquier etiqueta a las instancias y los volúmenes durante el lanzamiento. No se permite a los usuarios etiquetar ningún recurso (no pueden llamar directamente a la acción `ec2:CreateTags`).

```
{
```

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:region:account:*/*",
      "Condition": {
         "StringEquals": {
             "ec2:CreateAction" : "RunInstances"
          }
       }
    }
  ]
}
```

Igualmente, la siguiente política permite a los usuarios crear volúmenes y aplicar cualquier etiqueta a los volúmenes durante la creación de estos. No se permite a los usuarios etiquetar ningún recurso (no pueden llamar directamente a la acción `ec2:CreateTags`).

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateVolume"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:region:account:*/*",
      "Condition": {
```

```
          "StringEquals": {
              "ec2:CreateAction" : "CreateVolume"
           }
        }
     }
   ]
}
```

La acción `ec2:CreateTags` solo se evalúa si se aplican etiquetas durante la acción de creación de recursos. Por lo tanto, un usuario que tenga permisos para crear un recurso (suponiendo que no existan condiciones de etiquetado) no necesita permisos para utilizar la acción `ec2:CreateTags` si no se especifica ninguna etiqueta en la solicitud. Sin embargo, si el usuario intenta crear un recurso con etiquetas, la solicitud dará un error si el usuario no tiene permisos para utilizar la acción `ec2:CreateTags`.

La acción `ec2:CreateTags` también se evalúa si se proporcionan etiquetas en una plantilla de lanzamiento. Para ver una política de ejemplo, consulte Etiquetas en una plantilla de lanzamiento.

Controlar el acceso a etiquetas específicas

Puede utilizar condiciones adicionales en el elemento `Condition` de las políticas de IAM para controlar las claves y los valores de etiqueta que se pueden aplicar a los recursos.

Las siguientes claves de condición se pueden utilizar con los ejemplos de la sección anterior:

- `aws:RequestTag`: indicar que una clave de etiqueta o una clave y valor de etiqueta determinados deben existir en una solicitud. También se pueden especificar otras etiquetas en la solicitud.
  - Debe utilizarse con el operador de condición `StringEquals` para aplicar la combinación de valor y clave de etiqueta específica; por ejemplo, para aplicar la etiqueta `cost-center=cc123`:

    ```
    "StringEquals": { "aws:RequestTag/cost-center": "cc123" }
    ```

  - Debe utilizarse con el operador de condición `StringLike` para aplicar una clave de etiqueta específica en la solicitud; por ejemplo, para aplicar la clave de etiqueta `purpose`:

    ```
    "StringLike": { "aws:RequestTag/purpose": "*" }
    ```

- `aws:TagKeys`: aplicar las claves de etiqueta que se usan en la solicitud.
  - Debe utilizarse con el modificador `ForAllValues` para aplicar claves de etiqueta específicas si estas se proporcionan en la solicitud (si se especifican etiquetas en la solicitud, solo se permiten

claves de etiqueta específicas; no se permite ninguna etiqueta más). Por ejemplo, se permiten las claves de etiqueta `environment` o `cost-center`:

```
"ForAllValues:StringEquals": { "aws:TagKeys": ["environment","cost-center"] }
```

- Debe utilizarse con el modificador `ForAnyValue` para aplicar la presencia de como mínimo una de las claves de etiqueta especificadas en la solicitud. Por ejemplo, debe haber al menos una de las claves de etiqueta `environment` o `webserver` en la solicitud:

```
"ForAnyValue:StringEquals": { "aws:TagKeys": ["environment","webserver"] }
```

Estas claves de condición se pueden aplicar a las acciones que crean recursos y admiten el etiquetado, así como a las acciones `ec2:CreateTags` y `ec2:DeleteTags`. Para saber si una acción de la API de Amazon EC2 admite el etiquetado, consulte Acciones, recursos y claves de condición para Amazon EC2.

Para obligar a los usuarios a especificar etiquetas cuando crean un recurso, debe utilizar la clave de condición `aws:RequestTag` o la clave de condición `aws:TagKeys` con el modificador `ForAnyValue` en la acción de creación del recurso. La acción `ec2:CreateTags` no se evalúa si un usuario no especifica etiquetas para la acción de creación del recurso.

En cuanto a las condiciones, la clave de condición no distingue entre mayúsculas y minúsculas, mientras que el valor de condición sí. Por lo tanto, para aplicar la distinción entre mayúsculas y minúsculas de una clave de etiqueta, utilice la clave de condición `aws:TagKeys`, donde la clave de etiqueta se especifica como valor en la condición.

Para ver ejemplos de políticas de IAM, consulte Políticas de ejemplo para trabajar con la AWS CLI o un SDK de AWS. Para obtener más información sobre las condiciones con varios valores, consulte Creación de una condición que pruebe valores de varias claves en la Guía del usuario de IAM.

Control del acceso a recursos de EC2 mediante etiquetas de recursos

Cuando crea una política de IAM que concede a los usuarios permiso para utilizar recursos de EC2, puede incluir información de etiquetas en el elemento `Condition` de la política para controlar el acceso basado en etiquetas. Esto se conoce como control de acceso basado en atributos (ABAC). El ABAC le proporciona un mejor control sobre los recursos que un usuario puede modificar, utilizar o eliminar. Para obtener más información, consulte ¿Qué es ABAC para AWS?

Por ejemplo, puede crear una política que permita a los usuarios terminar una instancia, pero que deniegue la acción si la instancia tiene la etiqueta `environment=production`. Para ello, utilice la clave de condición `aws:ResourceTag` para permitir o denegar el acceso al recurso en función de las etiquetas que están asociadas al recurso.

```
"StringEquals": { "aws:ResourceTag/environment": "production" }
```

Para saber si una acción de la API de Amazon EC2 permite controlar el acceso mediante la clave de condición `aws:ResourceTag`, consulte Acciones, recursos y claves de condición para Amazon EC2. Tenga en cuenta que las acciones `Describe` no admiten permisos de nivel de recursos, de forma que debe especificarlas en una instrucción aparte sin condiciones.

Para ver ejemplos de políticas de IAM, consulte Políticas de ejemplo para trabajar con la AWS CLI o un SDK de AWS.

Si permite o deniega a los usuarios acceso a recursos en función de etiquetas, debe considerar denegar explícitamente a los usuarios la posibilidad de agregar estas etiquetas o retirarlas de los mismos recursos. De lo contrario, es posible que un usuario eluda sus restricciones y obtenga acceso a un recurso modificando sus etiquetas.

Políticas de ejemplo para trabajar con la AWS CLI o un SDK de AWS

Tiene que conceder a los usuarios los permisos que necesitan para Amazon EC2 mediante políticas de IAM. Los siguientes ejemplos muestran instrucciones de política que puede utilizar para controlar los permisos que los usuarios tienen en Amazon EC2. Estas políticas están diseñadas para solicitudes que se realizan con la AWS CLI o un SDK de AWS. Para obtener más información, consulte Creación de políticas de IAM en la Guía del usuario de IAM. Para ver políticas de ejemplo para trabajar en la consola de Amazon EC2, consulte Políticas de ejemplo para trabajar en la consola de Amazon EC2. Para obtener ejemplos de políticas de IAM específicas de Amazon VPC, consulte Identity and Access Management para Amazon VPC.

En los ejemplos siguientes, reemplace cada *`marcador de posición del usuario`* con su propia información.

Ejemplos

- Ejemplo: Acceso de solo lectura
- Ejemplo: Restringir el acceso a una región específica
- Trabajar con instancias

- Iniciar instancias (RunInstances)
- Trabajar con Instancias de spot
- Ejemplo: Trabajar con Instancias reservadas
- Ejemplo: Etiquetar recursos
- Ejemplo: Trabajar con roles de IAM
- Ejemplo: Trabajar con tablas de ruteo
- Ejemplo: Permitir que una instancia específica vea los recursos de otros servicios de AWS
- Ejemplo: Trabajar con plantillas de lanzamiento
- Trabajar con metadatos de instancias
- Uso de volúmenes e instantáneas de Amazon EBS

Ejemplo: Acceso de solo lectura

La siguiente política concede a los usuarios permisos para usar todas las acciones de la API de Amazon EC2 cuyos nombres empiecen por `Describe`. El elemento `Resource` utiliza un carácter comodín para indicar que los usuarios pueden especificar todos los recursos con estas acciones de API. El carácter comodín * también es necesario en los casos en los que la acción de la API no admita permisos de nivel de recursos. Para obtener más información acerca de qué ARN puede usar con qué acciones de la API de Amazon EC2, consulte Acciones, recursos y claves de condición para Amazon EC2.

Los usuarios no tienen permiso para realizar ninguna acción en los recursos (a menos que otra instrucción les de permiso para ello), porque, de forma predeterminada, se les deniega el permiso para usar acciones de la API.

```
{
   "Version": "2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource": "*"
    }
   ]
}
```

Ejemplo: Restringir el acceso a una región específica

La siguiente política deniega a los usuarios el permiso para usar todas las acciones de la API de Amazon EC2 a menos que la región sea Europa (Fráncfort). Utiliza la clave de condición global `aws:RequestedRegion`, que admiten todas las acciones de la API de Amazon EC2.

```
{
  "Version":"2012-10-17",
  "Statement": [
       {
      "Effect": "Deny",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": "eu-central-1"
        }
      }
    }
  ]
}
```

De forma alternativa, puede usar la clave de condición `ec2:Region`, que es específica de Amazon EC2 y que admiten todas las acciones de la API de Amazon EC2.

```
{
  "Version":"2012-10-17",
  "Statement": [
       {
      "Effect": "Deny",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "ec2:Region": "eu-central-1"
        }
      }
    }
  ]
}
```

Trabajar con instancias

Ejemplos

- Ejemplo: Describir, iniciar, detener, comenzar y terminar todas las instancias
- Ejemplo: Describir todas las instancias y detener, comenzar y terminar solo instancias determinadas

Ejemplo: Describir, iniciar, detener, comenzar y terminar todas las instancias

La siguiente política concede a los usuarios permisos para usar las acciones de la API especificadas en el elemento `Action`. El elemento `Resource` utiliza un carácter comodín * para indicar que los usuarios pueden especificar todos los recursos con estas acciones de API. El carácter comodín * también es necesario en los casos en los que la acción de la API no admita permisos de nivel de recursos. Para obtener más información acerca de qué ARN puede usar con qué acciones de la API de Amazon EC2, consulte Acciones, recursos y claves de condición para Amazon EC2.

Los usuarios no tienen permiso para utilizar cualquier otra acción de la API (a menos que otra instrucción les de permiso para ello), porque, de forma predeterminada, se les deniega el permiso para usar acciones de la API.

```
{
   "Version": "2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeAvailabilityZones",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "ec2:StopInstances",
        "ec2:StartInstances"
      ],
      "Resource": "*"
    }
   ]
}
```

Ejemplo: Describir todas las instancias y detener, comenzar y terminar solo instancias determinadas

La siguiente política permite a los usuarios describir todas las instancias, iniciar y detener únicamente las instancias i-1234567890abcdef0 y i-0598c7d356eba48d7, y terminar únicamente las instancias de la Región EE.UU. Este (Norte de Virginia) (`us-east-1`) con la etiqueta de recurso "`purpose=test`".

La primera instrucción utiliza un comodín * para el elemento `Resource` para indicar que los usuarios pueden especificar todos los recursos con la acción; en este caso, pueden generar una lista de todas las instancias. El carácter comodín * también es necesario en los casos en que la acción de la API no admite permisos de nivel de recursos (en este caso, `ec2:DescribeInstances`). Para obtener más información acerca de qué ARN puede usar con qué acciones de la API de Amazon EC2, consulte Acciones, recursos y claves de condición para Amazon EC2.

La segunda instrucción utiliza permisos de nivel de recursos para las acciones `StopInstances` y `StartInstances`. Las instancias específicas se indican mediante sus ARN en el elemento `Resource`.

La tercera instrucción permite a los usuarios terminar todas las instancias de la región Este de EE. UU. (Norte de Virginia) (`us-east-1`) que pertenezcan a la cuenta de AWS especificada, pero solo si la instancia tiene la etiqueta "`purpose=test`". El elemento `Condition` estipula cuando la instrucción de la política está en vigor.

```
{
   "Version": "2012-10-17",
   "Statement": [
   {
   "Effect": "Allow",
      "Action": "ec2:DescribeInstances",
      "Resource": "*"
   },
   {
      "Effect": "Allow",
      "Action": [
        "ec2:StopInstances",
        "ec2:StartInstances"
      ],
      "Resource": [
        "arn:aws:ec2:us-east-1:account-id:instance/i-1234567890abcdef0",
        "arn:aws:ec2:us-east-1:account-id:instance/i-0598c7d356eba48d7"
      ]
```

```
    },
    {
      "Effect": "Allow",
      "Action": "ec2:TerminateInstances",
      "Resource": "arn:aws:ec2:us-east-1:account-id:instance/*",
      "Condition": {
         "StringEquals": {
            "aws:ResourceTag/purpose": "test"
         }
      }
   }

   ]
}
```

Iniciar instancias (RunInstances)

La acción de la API RunInstances lanza una o varias Instancias bajo demanda o una o varias Instancias de spot. `RunInstances` requiere una AMI y crea una instancia. Los usuarios pueden especificar un par de claves y un grupo de seguridad en la solicitud. El lanzamiento en una VPC requiere una subred y crea una interfaz de red. El lanzamiento desde una AMI con respaldo de Amazon EBS crea un volumen. Por lo tanto, el usuario debe tener permisos para usar estos recursos de Amazon EC2. Puede crear una instrucción de política que exija a los usuarios que especifiquen un parámetro opcional en `RunInstances` o que restrinja los valores de un parámetro a valores determinados.

Para obtener más información sobre los permisos de nivel de recurso necesarios para iniciar una instancia, consulte Claves de condición, acciones y recursos de Amazon EC2.

De forma predeterminada, los usuarios no tienen permisos para describir, comenzar, detener o terminar las instancias resultantes. Una de las posibles maneras de conceder a los usuarios permisos para administrar las instancias obtenidas consiste en crear una etiqueta específica para cada instancia y, a continuación, crear una instrucción que les permita administrar instancias con dicha etiqueta. Para obtener más información, consulte Trabajar con instancias.

Recursos

- AMI
- Tipos de instancias
- Subredes
- Volúmenes de EBS

- Etiquetas
- Etiquetas en una plantilla de lanzamiento
- GPU elásticas
- Plantillas de lanzamiento

AMI

La siguiente política permite a los usuarios iniciar instancias utilizando únicamente las AMI especificadas, `ami-9e1670f7` y `ami-45cf5c3c`. Los usuarios no pueden lanzar una instancia con otras AMI (a menos que otra instrucción conceda a los usuarios permiso para ello).

```
{
   "Version": "2012-10-17",
   "Statement": [
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:region::image/ami-9e1670f7",
        "arn:aws:ec2:region::image/ami-45cf5c3c",
        "arn:aws:ec2:region:account-id:instance/*",
        "arn:aws:ec2:region:account-id:volume/*",
        "arn:aws:ec2:region:account-id:key-pair/*",
        "arn:aws:ec2:region:account-id:security-group/*",
        "arn:aws:ec2:region:account-id:subnet/*",
        "arn:aws:ec2:region:account-id:network-interface/*"
      ]
    }
   ]
}
```

Como alternativa, la siguiente política permite a los usuarios iniciar instancias desde todas las AMI propiedad de Amazon o de determinados socios verificados y de confianza. El elemento `Condition` de la primera instrucción prueba si `ec2:Owner` es `amazon`. Los usuarios no pueden lanzar una instancia con otras AMI (a menos que otra instrucción conceda a los usuarios permiso para ello).

```
{
   "Version": "2012-10-17",
   "Statement": [
         {
```

```
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region::image/ami-*"
      ],
      "Condition": {
         "StringEquals": {
            "ec2:Owner": "amazon"
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region:account-id:instance/*",
         "arn:aws:ec2:region:account-id:subnet/*",
         "arn:aws:ec2:region:account-id:volume/*",
         "arn:aws:ec2:region:account-id:network-interface/*",
         "arn:aws:ec2:region:account-id:key-pair/*",
         "arn:aws:ec2:region:account-id:security-group/*"
         ]
      }
   ]
}
```

Tipos de instancias

La siguiente política permite a los usuarios iniciar instancias utilizando únicamente el tipo de instancia `t2.micro` o `t2.small`, que usted podría utilizar para controlar costos. Los usuarios no pueden iniciar instancias más grandes porque el elemento `Condition` de la primera instrucción prueba si `ec2:InstanceType` es `t2.micro` o `t2.small`.

```
{
   "Version": "2012-10-17",
   "Statement": [
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region:account-id:instance/*"
      ],
      "Condition": {
```

```
         "StringEquals": {
            "ec2:InstanceType": ["t2.micro", "t2.small"]
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region::image/ami-*",
         "arn:aws:ec2:region:account-id:subnet/*",
         "arn:aws:ec2:region:account-id:network-interface/*",
         "arn:aws:ec2:region:account-id:volume/*",
         "arn:aws:ec2:region:account-id:key-pair/*",
         "arn:aws:ec2:region:account-id:security-group/*"
         ]
      }
   ]
}
```

Como alternativa, puede crear una política que deniegue a los usuarios permisos para iniciar instancias, salvo los tipos de instancias `t2.micro` y `t2.small`.

```
{
   "Version": "2012-10-17",
   "Statement": [
        {
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region:account-id:instance/*"
      ],
      "Condition": {
         "StringNotEquals": {
            "ec2:InstanceType": ["t2.micro", "t2.small"]
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region::image/ami-*",
```

```
            "arn:aws:ec2:region:account-id:network-interface/*",
            "arn:aws:ec2:region:account-id:instance/*",
            "arn:aws:ec2:region:account-id:subnet/*",
            "arn:aws:ec2:region:account-id:volume/*",
            "arn:aws:ec2:region:account-id:key-pair/*",
            "arn:aws:ec2:region:account-id:security-group/*"
            ]
      }
   ]
}
```

Subredes

La siguiente política permite a los usuarios iniciar instancias utilizando únicamente la subred especificada, `subnet-12345678`. El grupo no puede iniciar instancias en cualquier otra subred (a menos que otra instrucción conceda a los usuarios permiso para ello).

```
{
   "Version": "2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:region:account-id:subnet/subnet-12345678",
        "arn:aws:ec2:region:account-id:network-interface/*",
        "arn:aws:ec2:region:account-id:instance/*",
        "arn:aws:ec2:region:account-id:volume/*",
        "arn:aws:ec2:region::image/ami-*",
        "arn:aws:ec2:region:account-id:key-pair/*",
        "arn:aws:ec2:region:account-id:security-group/*"
      ]
    }
   ]
}
```

Como alternativa, puede crear una política que deniegue a los usuarios permisos para iniciar una instancia en cualquier otra subred. La instrucción actúa así denegando el permiso para crear una interfaz de red, salvo en la ubicación donde la subred `subnet-12345678` está especificada. Esta denegación anula cualquier otra política creada para permitir el lanzamiento de instancias en otras subredes.

```
{
   "Version": "2012-10-17",
   "Statement": [
         {
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region:account-id:network-interface/*"
      ],
      "Condition": {
         "ArnNotEquals": {
            "ec2:Subnet": "arn:aws:ec2:region:account-id:subnet/subnet-12345678"
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region::image/ami-*",
         "arn:aws:ec2:region:account-id:network-interface/*",
         "arn:aws:ec2:region:account-id:instance/*",
         "arn:aws:ec2:region:account-id:subnet/*",
         "arn:aws:ec2:region:account-id:volume/*",
         "arn:aws:ec2:region:account-id:key-pair/*",
         "arn:aws:ec2:region:account-id:security-group/*"
         ]
      }
   ]
}
```

Volúmenes de EBS

La siguiente política permite a los usuarios iniciar instancias únicamente si los volúmenes EBS de la instancia están cifrados. El usuario debe iniciar una instancia desde una AMI que se creó con instantáneas cifradas para garantizar el cifrado del volumen raíz. Cualquier volumen adicional que el usuario adjunte a la instancia durante el lanzamiento también debe estar cifrado.

```
{
    "Version": "2012-10-17",
    "Statement": [
                {
```

```
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Condition": {
                "Bool": {
                    "ec2:Encrypted": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:*::image/ami-*",
                "arn:aws:ec2:*:*:network-interface/*",
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ec2:*:*:subnet/*",
                "arn:aws:ec2:*:*:key-pair/*",
                "arn:aws:ec2:*:*:security-group/*"
            ]
        }
    ]
}
```

Etiquetas

Etiquetar instancias durante la creación

La siguiente política permite a los usuarios iniciar instancias y etiquetarlas durante la creación. En las acciones de creación de recursos que aplican etiquetas, los usuarios deben tener permisos para utilizar la acción `CreateTags`. La segunda instrucción utiliza la clave de condición `ec2:CreateAction` para permitir a los usuarios crear etiquetas únicamente en el contexto de `RunInstances` y solo para instancias. Los usuarios no pueden etiquetar recursos ya existentes ni tampoco etiquetar volúmenes utilizando la solicitud `RunInstances`.

Para obtener más información, consulte Conceder permisos para etiquetar recursos durante la creación.

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:account-id:instance/*",
      "Condition": {
         "StringEquals": {
             "ec2:CreateAction" : "RunInstances"
          }
       }
    }
  ]
}
```

Etiquetar instancias y volúmenes durante la creación con etiquetas específicas

La siguiente política contiene la clave de condición `aws:RequestTag` que exige a los usuarios que etiqueten todas las instancias que se creen con `RunInstances`, con las etiquetas `environment=production` y `purpose=webserver`. Si los usuarios no transmiten estas etiquetas en concreto o si no especifican ninguna etiqueta, la solicitud dará un error.

```
{
  "Version": "2012-10-17",
  "Statement": [
   {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": [
         "arn:aws:ec2:region::image/*",
         "arn:aws:ec2:region:account-id:subnet/*",
         "arn:aws:ec2:region:account-id:network-interface/*",
         "arn:aws:ec2:region:account-id:security-group/*",
         "arn:aws:ec2:region:account-id:key-pair/*"
```

```
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": [
          "arn:aws:ec2:region:account-id:volume/*",
          "arn:aws:ec2:region:account-id:instance/*"
      ],
      "Condition": {
         "StringEquals": {
             "aws:RequestTag/environment": "production" ,
             "aws:RequestTag/purpose": "webserver"
          }
       }
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:region:account-id:*/*",
      "Condition": {
         "StringEquals": {
             "ec2:CreateAction" : "RunInstances"
          }
       }
    }
  ]
}
```

Etiquetar instancias y volúmenes durante la creación con al menos una etiqueta específica

La siguiente política utiliza el modificador `ForAnyValue` en la condición `aws:TagKeys` para indicar que debe especificarse como mínimo una etiqueta en la solicitud y que esta debe contener la clave `environment` o `webserver`. La etiqueta debe aplicarse tanto a las instancias como a los volúmenes. Se puede especificar cualquier valor de etiqueta en la solicitud.

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
    {
       "Effect": "Allow",
       "Action": [
          "ec2:RunInstances"
       ],
       "Resource": [
          "arn:aws:ec2:region::image/*",
          "arn:aws:ec2:region:account-id:subnet/*",
          "arn:aws:ec2:region:account-id:network-interface/*",
          "arn:aws:ec2:region:account-id:security-group/*",
          "arn:aws:ec2:region:account-id:key-pair/*"
       ]
     },
     {
       "Effect": "Allow",
       "Action": [
           "ec2:RunInstances"
       ],
       "Resource": [
           "arn:aws:ec2:region:account-id:volume/*",
           "arn:aws:ec2:region:account-id:instance/*"
       ],
       "Condition": {
           "ForAnyValue:StringEquals": {
               "aws:TagKeys": ["environment","webserver"]
           }
        }
     },
     {
       "Effect": "Allow",
       "Action": [
           "ec2:CreateTags"
       ],
       "Resource": "arn:aws:ec2:region:account-id:*/*",
       "Condition": {
           "StringEquals": {
               "ec2:CreateAction" : "RunInstances"
           }
        }
     }
   ]
}
```

Si las instancias se etiquetan durante la creación, deben etiquetarse con una etiqueta específica

En la siguiente política, los usuarios no tienen que especificar etiquetas en la solicitud, pero si lo hacen, la etiqueta tiene que ser `purpose=test`. No se permite ninguna otra etiqueta. Los usuarios pueden aplicar etiquetas a todos los recursos de la solicitud `RunInstances` que lo admitan.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:region:account-id:*/*",
      "Condition": {
         "StringEquals": {
             "aws:RequestTag/purpose": "test",
             "ec2:CreateAction" : "RunInstances"
          },
          "ForAllValues:StringEquals": {
              "aws:TagKeys": "purpose"
          }
       }
    }
  ]
}
```

Para no permitir ninguna etiqueta llamada al crear para RunInstances

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
```

```
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "VisualEditor0",
            "Effect": "Deny",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Permitir solo etiquetas específicas para spot-instances-request. La incoherencia sorpresa número 2 entra en juego aquí. En circunstancias normales, no especificar ninguna etiqueta dará como resultado No autenticado. En el caso de spot-instances-request, esta política no se evaluará si no hay etiquetas spot-instances-request, por lo que una solicitud Subasta en ejecución sin etiqueta tendrá éxito.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
```

```
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
            ]
        },
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1:*:spot-instances-request/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": "production"
                }
            }
        }
    ]
}
```

Etiquetas en una plantilla de lanzamiento

En el siguiente ejemplo, los usuarios pueden lanzar instancias, pero solo si usan una plantilla de lanzamiento específica (`lt-09477bcd97b0d310e`). La clave de condición `ec2:IsLaunchTemplateResource` evita que los usuarios invaliden cualquiera de los recursos especificados en la plantilla de lanzamiento. La segunda parte de la instrucción permite a los usuarios etiquetar instancias en el momento de la creación — Esta parte es necesaria si se especifican las etiquetas para la instancia en la plantilla de lanzamiento.

```
{
  "Version": "2012-10-17",
  "Statement": [
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "*",
      "Condition": {
         "ArnLike": {
             "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/
lt-09477bcd97b0d310e"
          },
          "Bool": {
```

```
            "ec2:IsLaunchTemplateResource": "true"
          }
       }
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:region:account-id:instance/*",
      "Condition": {
         "StringEquals": {
             "ec2:CreateAction" : "RunInstances"
          }
       }
    }
  ]
}
```

GPU elásticas

En la siguiente política, los usuarios pueden iniciar una instancia y especificar la GPU elástica que se va a asociar a la instancia. Los usuarios pueden iniciar instancias en cualquier región, pero solo pueden conectar una GPU elástica durante un lanzamiento en la región `us-east-2`.

La clave de condición `ec2:ElasticGpuType` garantiza que las instancias usen el tipo de GPU elástico `eg1.medium` o `eg1.large`.

```
{
    "Version": "2012-10-17",
    "Statement": [
             {
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:*:account-id:elastic-gpu/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:Region": "us-east-2",
                    "ec2:ElasticGpuType": [
```

```
                        "eg1.medium",
                        "eg1.large"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:*::image/ami-*",
                "arn:aws:ec2:*:account-id:network-interface/*",
                "arn:aws:ec2:*:account-id:instance/*",
                "arn:aws:ec2:*:account-id:subnet/*",
                "arn:aws:ec2:*:account-id:volume/*",
                "arn:aws:ec2:*:account-id:key-pair/*",
                "arn:aws:ec2:*:account-id:security-group/*"
            ]
        }
    ]
}
```

Plantillas de lanzamiento

En el siguiente ejemplo, los usuarios pueden lanzar instancias, pero solo si usan una plantilla de lanzamiento específica (`lt-09477bcd97b0d310e`). Los usuarios pueden omitir parámetros de la plantilla de lanzamiento al especificarlos en la acción `RunInstances`.

```
{
  "Version": "2012-10-17",
  "Statement": [
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "*",
      "Condition": {
         "ArnLike": {
            "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/
lt-09477bcd97b0d310e"
          }
       }
    }
  ]
```

```
}
```

En este ejemplo, los usuarios pueden iniciar instancias, pero solo si usan una plantilla de lanzamiento. La política usa la clave de condición `ec2:IsLaunchTemplateResource` para evitar que los usuarios invaliden cualquiera de los ARN preexistentes de la plantilla de lanzamiento.

```
{
  "Version": "2012-10-17",
  "Statement": [
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "*",
      "Condition": {
         "ArnLike": {
             "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/*"
          },
          "Bool": {
             "ec2:IsLaunchTemplateResource": "true"
          }
       }
    }
  ]
}
```

En el siguiente ejemplo, la política permite a los usuarios iniciar instancias, pero solo si usan una plantilla de lanzamiento. Los usuarios no pueden omitir los parámetros de subred y de interfaz de red de la solicitud; estos parámetros solo pueden especificarse en la plantilla de lanzamiento. La primera parte de la instrucción utiliza el elemento NotResource para permitir todos los demás recursos, excepto las subredes y las interfaces de red. La segunda parte de la instrucción permite los recursos de subred y de interfaz de red, pero solo si provienen de la plantilla de lanzamiento.

```
{
  "Version": "2012-10-17",
  "Statement": [
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "NotResource": ["arn:aws:ec2:region:account-id:subnet/*",
                      "arn:aws:ec2:region:account-id:network-interface/*" ],
      "Condition": {
         "ArnLike": {
```

```
            "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/*"
          }
       }
    },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": ["arn:aws:ec2:region:account-id:subnet/*",
                   "arn:aws:ec2:region:account-id:network-interface/*" ],
      "Condition": {
         "ArnLike": {
            "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/*"
          },
          "Bool": {
            "ec2:IsLaunchTemplateResource": "true"
          }
       }
    }
  ]
}
```

En el siguiente ejemplo, se le permite a los usuarios iniciar instancias solo si usan una plantilla de lanzamiento que contenga la etiqueta `Purpose=Webservers`. Los usuarios no pueden omitir ninguno de los parámetros de la plantilla de lanzamiento en la acción `RunInstances`.

```
{
  "Version": "2012-10-17",
  "Statement": [
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "NotResource": "arn:aws:ec2:region:account-id:launch-template/*",
      "Condition": {
         "ArnLike": {
            "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/*"
          },
         "Bool": {
            "ec2:IsLaunchTemplateResource": "true"
          }
       }
    },
    {
      "Effect": "Allow",
```

```
      "Action": "ec2:RunInstances",
      "Resource": "arn:aws:ec2:region:account-id:launch-template/*",
      "Condition": {
       "StringEquals": {
           "aws:ResourceTag/Purpose": "Webservers"
        }
       }
     }
  ]
}
```

Trabajar con Instancias de spot

Puede utilizar la acción RunInstances para crear solicitudes de instancias de spot y etiquetarlas durante la creación. El recurso que se debe especificar para RunInstances es `spot-instances-request`.

El recurso `spot-instances-request` se evalúa en la política de IAM de la siguiente manera:

- Si no etiqueta la solicitud de instancia de spot durante la creación, Amazon EC2 no evalúa el recurso `spot-instances-request` en la instrucción RunInstances.
- Si etiqueta la solicitud de instancia de spot durante la creación, Amazon EC2 evalúa el recurso `spot-instances-request` en la instrucción RunInstances.

Por lo tanto, para el recurso `spot-instances-request`, se aplican las siguientes reglas a la política de IAM:

- Si utiliza RunInstances para crear una solicitud de instancia de spot y no tiene la intención de etiquetar dicha solicitud durante la creación, no es necesario que permita explícitamente el recurso `spot-instances-request`; la llamada se realizará correctamente.
- Si utiliza RunInstances para crear una solicitud de instancia de spot y tiene la intención de etiquetar dicha solicitud durante la creación, debe incluir el recurso `spot-instances-request` en la instrucción de permiso de RunInstances; de lo contrario, la llamada devolverá un error.
- Si utiliza RunInstances para crear una solicitud de instancia de spot y tiene la intención de etiquetar dicha solicitud durante la creación, debe especificar el recurso `spot-instances-request` o incluir el comodín `*` en la instrucción de permiso de CreateTags; de lo contrario, la llamada devolverá un error.

Puede solicitar Instancias de spot mediante RunInstances o RequestSpotInstances. Las siguientes políticas de IAM de ejemplo siguientes solo se aplican cuando se solicita Instancias de spot mediante RunInstances.

Ejemplo: solicitud de Instancias de spot mediante RunInstances

La siguiente política permite a los usuarios solicitar Instancias de spot mediante la acción RunInstances. El recurso `spot-instances-request`, creado por RunInstances, solicita Instancias de spot.

> **Note**
>
> Si va a utilizar RunInstances para crear solicitudes de instancias de spot, puede omitir `spot-instances-request` de la lista `Resource` si no tiene la intención de etiquetar las solicitudes de instancias de spot durante la creación. Esto se debe a que Amazon EC2 no evalúa el recurso `spot-instances-request` en la instrucción RunInstances si la solicitud de instancia de spot no se etiqueta durante la creación.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        }
    ]
}
```

Warning

NO ADMITIDO: ejemplo: denegar permiso a los usuarios para solicitar Instancias de spot utilizando RunInstances

No se admite la política siguiente para el recurso `spot-instances-request`.

La siguiente política tiene por objeto conceder a los usuarios el permiso para iniciar Instancias bajo demanda, pero denegar a los usuarios el permiso para solicitar Instancias de spot. El recurso `spot-instances-request`, creado por RunInstances, es el recurso que solicita Instancias de spot. La segunda instrucción tiene por objeto denegar la acción RunInstances para el recurso `spot-instances-request`. Sin embargo, no se admite esta condición porque Amazon EC2 no evalúa el recurso `spot-instances-request` en la instrucción RunInstances si la solicitud de instancia de spot no se etiqueta durante la creación.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*"
            ]
        },
        {
            "Sid": "DenySpotInstancesRequests - NOT SUPPORTED - DO NOT USE!",
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
        }
    ]
```

```
}
```

Ejemplo: etiquetar solicitudes de instancias de spot durante la creación

La siguiente política permite a los usuarios etiquetar todos los recursos que se crean durante el lanzamiento de la instancia. La primera instrucción permite a RunInstances crear los recursos enumerados. El recurso `spot-instances-request`, creado por RunInstances, es el recurso que solicita Instancias de spot. La segunda instrucción proporciona un comodín * para permitir que se etiqueten todos los recursos cuando se crean durante el lanzamiento de la instancia.

> **Note**
>
> Si etiqueta la solicitud de instancia de spot durante la creación, Amazon EC2 evalúa el recurso `spot-instances-request` en la instrucción RunInstances. Por lo tanto, debe permitir explícitamente el recurso `spot-instances-request` para la acción RunInstances; de lo contrario, la llamada devolverá un error.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
```

```
            "Sid": "TagResources",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Ejemplo: denegar el etiquetado durante la creación para solicitudes de instancias de spot

La política siguiente deniega a los usuarios el permiso para etiquetar los recursos que se crean durante el lanzamiento de la instancia.

La primera instrucción permite a RunInstances crear los recursos enumerados. El recurso `spot-instances-request`, creado por RunInstances, es el recurso que solicita Instancias de spot. La segunda instrucción proporciona un comodín `*` para denegar todos los recursos que se etiquetan cuando se crean durante el lanzamiento de la instancia. Si `spot-instances-request` o cualquier otro recurso se etiqueta durante la creación, la llamada RunInstances devolverá un error.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "DenyTagResources",
            "Effect": "Deny",
            "Action": "ec2:CreateTags",
```

```
            "Resource": "*"
        }
    ]
}
```

Warning

NO ADMITIDO – Ejemplo: permitir la creación de una solicitud de instancia de spot solo si se le asigna una etiqueta específica

No se admite la política siguiente para el recurso `spot-instances-request`.

La siguiente política tiene por objeto otorgar a RunInstances el permiso para crear una solicitud de instancia de spot solo si la solicitud se etiqueta con una etiqueta específica.

La primera instrucción permite a RunInstances crear los recursos enumerados.

La segunda instrucción tiene por objeto otorgar a los usuarios el permiso para crear una solicitud de instancia de spot solo si la solicitud tiene la etiqueta `environment=production`. Si esta condición se aplica a los demás recursos creados por RunInstances, si no se especifica ninguna etiqueta se producirá un error `Unauthenticated`. Sin embargo, si no se especifica ninguna etiqueta para la solicitud de instancia de spot, Amazon EC2 no evalúa el recurso `spot-instances-request` en la instrucción RunInstances, lo que da como resultado que RunInstances cree solicitudes de instancias de spot no etiquetadas.

Tenga en cuenta que especificar una etiqueta que no sea `environment=production` da como resultado un error `Unauthenticated`, ya que si un usuario etiqueta una solicitud de instancia de spot, Amazon EC2 evalúa el recurso `spot-instances-request` en la instrucción RunInstances.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
```

```
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*"
            ]
        },
        {
            "Sid": "RequestSpotInstancesOnlyIfTagIs_environment=production - NOT
 SUPPORTED - DO NOT USE!",
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1:*:spot-instances-request/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": "production"
                }
            }
        },
        {
            "Sid": "TagResources",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }

    ]
}
```

Ejemplo: denegar la creación de una solicitud de instancia de spot si se le asigna una etiqueta específica

La siguiente política deniega a RunInstances el permiso para crear una solicitud de instancia de spot si la solicitud está etiquetada con `environment=production`.

La primera instrucción permite a RunInstances crear los recursos enumerados.

La segunda instrucción deniega a los usuarios el permiso para crear una solicitud de instancia de spot si la solicitud tiene la etiqueta `environment=production`. Si `environment=production` se especifica como etiqueta, se produce un error `Unauthenticated`. Especificar otras etiquetas o no especificar ninguna etiqueta dará como resultado la creación de una solicitud de instancia de spot.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "DenySpotInstancesRequests",
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1:*:spot-instances-request/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": "production"
                }
            }
        },
        {
            "Sid": "TagResources",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Ejemplo: Trabajar con Instancias reservadas

La siguiente política da a los usuarios permiso para ver, modificar y adquirir Instancias reservadas en su cuenta.

No se pueden establecer permisos de nivel de recursos para Instancias reservadas individuales. Esta política significa que los usuarios tienen acceso a todas las Instancias reservadas de la cuenta.

El elemento `Resource` utiliza un comodín * para indicar que los usuarios pueden especificar todos los recursos con la acción; en dicho caso, pueden generar una lista y modificar todas las Instancias reservadas de la cuenta. También pueden adquirir Instancias reservadas utilizando las credenciales de cuenta. El carácter comodín * también es necesario en los casos en los que la acción de la API no admita permisos de nivel de recursos.

```
{
   "Version": "2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeReservedInstances",
        "ec2:ModifyReservedInstances",
        "ec2:PurchaseReservedInstancesOffering",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeReservedInstancesOfferings"
      ],
      "Resource": "*"
    }
   ]
}
```

Para permitir a los usuarios ver y modificar las Instancias reservadas de su cuenta, pero no adquirir otras Instancias reservadas nuevas.

```
{
  "Version": "2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeReservedInstances",
```

```
        "ec2:ModifyReservedInstances",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource": "*"
    }
  ]
}
```

Ejemplo: Etiquetar recursos

La siguiente política permite a los usuarios utilizar la acción `CreateTags` para aplicar etiquetas a una instancia solo si la etiqueta contiene la clave `environment` y el valor `production`. No se permite ninguna otra etiqueta y el usuario no puede etiquetar ningún otro tipo de recurso.

```
{
    "Version": "2012-10-17",
    "Statement": [
              {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:region:account-id:instance/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": "production"
                }
            }
        }
    ]
}
```

La siguiente política permite a los usuarios etiquetar cualquier recurso etiquetable que ya tenga una etiqueta con una clave de `owner` y un valor del nombre de usuario. Asimismo, los usuarios deben especificar una etiqueta con una clave de `anycompany:environment-type` y un valor que sea `test` o `prod` en la solicitud. Los usuarios pueden especificar más etiquetas en la solicitud.

```
{
    "Version": "2012-10-17",
    "Statement": [
              {
```

```
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:region:account-id:*/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/anycompany:environment-type": ["test","prod"],
                    "aws:ResourceTag/owner": "${aws:username}"
                }
            }
        }
    ]
}
```

Puede crear una política de IAM que permita a los usuarios eliminar etiquetas específicas de un recurso. Por ejemplo, la siguiente política permite a los usuarios eliminar etiquetas de un volumen si las claves de etiqueta especificadas en la solicitud son `environment` o `cost-center`. Se puede especificar cualquier valor para la etiqueta, pero la clave de etiqueta debe coincidir con una de las dos claves indicadas.

> **Note**
>
> Si elimina un recurso, también se eliminarán todas las etiquetas que este tenga asociadas. Los usuarios no necesitan permisos para utilizar la acción `ec2:DeleteTags` para eliminar un recurso que tenga etiquetas; solo los necesitan para realizar la acción de eliminación.

```
{
  "Version": "2012-10-17",
  "Statement": [
       {
      "Effect": "Allow",
      "Action": "ec2:DeleteTags",
      "Resource": "arn:aws:ec2:us-east-1:account-id:volume/*",
      "Condition": {
        "ForAllValues:StringEquals": {
          "aws:TagKeys": ["environment","cost-center"]
        }
      }
    }
```

```
  ]
}
```

Esta política permite a los usuarios eliminar únicamente la etiqueta `environment=prod` en cualquier recurso solo si el recurso ya está etiquetado con la clave de `owner` y un valor del nombre de usuario. Los usuarios no pueden eliminar ninguna etiqueta de recurso más.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteTags"
      ],
      "Resource": "arn:aws:ec2:region:account-id:*/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/environment": "prod",
          "aws:ResourceTag/owner": "${aws:username}"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": ["environment"]
        }
      }
    }
  ]
}
```

Ejemplo: Trabajar con roles de IAM

La siguiente política permite a los usuarios asociar, sustituir y desasociar un rol de IAM a instancias que tienen la etiqueta `department=test`. Para sustituir o desasociar un rol de IAM, se necesita un ID de asociación, por lo que la política también concede a los usuarios permiso para utilizar la acción `ec2:DescribeIamInstanceProfileAssociations`.

Los usuarios deben tener permiso para utilizar la acción `iam:PassRole` con objeto de poder pasar el rol a la instancia.

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation",
        "ec2:DisassociateIamInstanceProfile"
      ],
      "Resource": "arn:aws:ec2:us-east-1:account-id:instance/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/department":"test"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:DescribeIamInstanceProfileAssociations",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::account-id:role/DevTeam*"
    }
  ]
}
```

La siguiente política permite a los usuarios adjuntar o reemplazar un rol de IAM para cualquier instancia. Los usuarios solo pueden asociar o sustituir roles de IAM con nombres que empiecen por `TestRole-`. En el caso de la acción `iam:PassRole`, asegúrese de especificar el nombre del rol de IAM y no el perfil de instancia (si los nombres son diferentes). Para obtener más información, consulte Perfiles de instancias.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AssociateIamInstanceProfile",
                "ec2:ReplaceIamInstanceProfileAssociation"
            ],
```

```
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeIamInstanceProfileAssociations",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::account-id:role/TestRole-*"
        }
    ]
}
```

Ejemplo: Trabajar con tablas de ruteo

La siguiente política permite a los usuarios añadir, eliminar y reemplazar rutas únicamente para las tablas de ruteo que están asociadas a la VPC `vpc-ec43eb89`. Para especificar una VPC para la clave de condición `ec2:Vpc`, debe especificar el ARN completo de la VPC.

```
{
    "Version": "2012-10-17",
    "Statement": [
              {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteRoute",
                "ec2:CreateRoute",
                "ec2:ReplaceRoute"
            ],
            "Resource": [
                "arn:aws:ec2:region:account-id:route-table/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:Vpc": "arn:aws:ec2:region:account-id:vpc/vpc-ec43eb89"
                }
            }
        }
    ]
}
```

Ejemplo: Permitir que una instancia específica vea los recursos de otros servicios de AWS

El siguiente es un ejemplo de una política que puede asociar a un rol de IAM. La política permite que una instancia vea los recursos de diversos servicios de AWS. Usa la clave de condición `ec2:SourceInstanceARN` para especificar que la instancia desde la que se realiza la solicitud debe ser `i-093452212644b0dd6`. Si el mismo rol de IAM está asociado a otra instancia, la otra instancia no puede realizar ninguna de estas acciones.

La clave `ec2:SourceInstanceARN` es una clave de condición global de AWS y, por lo tanto, se puede usar para otras acciones de servicios, no solo para Amazon EC2.

```
{
    "Version": "2012-10-17",
    "Statement": [
              {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVolumes",
                "s3:ListAllMyBuckets",
                "dynamodb:ListTables",
                "rds:DescribeDBInstances"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "ArnEquals": {
                    "ec2:SourceInstanceARN": "arn:aws:ec2:region:account-id:instance/
i-093452212644b0dd6"
                }
            }
        }
    ]
}
```

Ejemplo: Trabajar con plantillas de lanzamiento

La siguiente política permite a los usuarios crear una versión de una plantilla de lanzamiento y modificar una plantilla de lanzamiento, pero solo para la plantilla de lanzamiento `lt-09477bcd97b0d3abc`. Los usuarios no pueden trabajar con otras plantillas de lanzamiento.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
   {
      "Action": [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:ec2:region:account-id:launch-template/lt-09477bcd97b0d3abc"
    }
  ]
}
```

La siguiente política permite a los usuarios eliminar cualquier plantilla de lanzamiento o versión de la misma, siempre que contenga la etiqueta `Purpose=Testing`.

```
{
  "Version": "2012-10-17",
  "Statement": [
       {
      "Action": [
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:ec2:region:account-id:launch-template/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Purpose": "Testing"
        }
      }
    }
  ]
}
```

Trabajar con metadatos de instancias

Las políticas siguientes garantizan que los usuarios solo puedan recuperar metadatos de instancias mediante Servicio de metadatos de instancia, versión 2 (IMDSv2). Puede combinar las cuatro políticas siguientes en una sola política con cuatro instrucciones. Cuando se combina como una sola política, puede utilizar la política como una política de control de servicios (SCP). Puede funcionar igual de bien que una política de denegación que se aplique a una política de IAM existente

(quitando y limitando los permisos existentes) o como una SCP que se aplique globalmente a una cuenta, una unidad organizativa (OU) o una organización completa.

> **Note**
>
> Las siguientes políticas de opciones de metadatos de RunInstances se deben utilizar junto con una política que conceda a la entidad principal permisos para iniciar una instancia con RunInstances. Si la entidad principal no tiene permisos RunInstances, no podrá iniciar una instancia. Para obtener más información, consulte las políticas en Trabajar con instancias y Iniciar instancias (RunInstances).

> **Important**
>
> Si utiliza grupos de Auto Scaling y necesita exigir el uso de IMDSv2 en todas las instancias nuevas, los grupos de Auto Scaling deben usar plantillas de lanzamiento.
> Cuando un grupo de Auto Scaling utiliza una plantilla de lanzamiento, los permisos `ec2:RunInstances` de la entidad principal de IAM se comprueban cuando se crea un nuevo grupo de Auto Scaling. También se comprueban cuando se actualiza un grupo de Auto Scaling existente para utilizar una nueva plantilla de lanzamiento o una nueva versión de una plantilla de lanzamiento.
> Las restricciones sobre el uso de IMDSv1 en entidades principales de IAM para `RunInstances` solo se comprueban cuando se crea o actualiza un grupo de Auto Scaling que utiliza una plantilla de lanzamiento. Para un grupo de Auto Scaling configurado para usar la plantilla de lanzamiento `Latest` o `Default`, los permisos no se comprueban cuando se crea una nueva versión de la plantilla de lanzamiento. Para que se comprueben los permisos, debe configurar el grupo de Auto Scaling para que utilice una versión específica de la plantilla de lanzamiento.
>
> Para forzar el uso de IMDSv2 en instancias lanzadas por grupos de Auto Scaling, se requieren los siguientes pasos adicionales:
>
> 1. Deshabilite el uso de configuraciones de lanzamiento para todas las cuentas de la organización mediante políticas de control de servicios (SCP) o límites de permisos de IAM para las nuevas entidades principales que se crean. Para las entidades principales de IAM existentes con permisos de grupos de Auto Scaling, actualice sus políticas asociadas con esta clave de condición. Para deshabilitar el uso de configuraciones de lanzamiento, cree o modifique la SCP, el límite de permisos o la política de IAM correspondientes

con la clave de condición `"autoscaling:LaunchConfigurationName"` con el valor especificado como `null`.

2. Para las nuevas plantillas de lanzamiento, configure las opciones de metadatos de la instancia en la plantilla de lanzamiento. Para las plantillas de lanzamiento existentes, cree una nueva versión de la plantilla de lanzamiento y configure las opciones de metadatos de la instancia en la nueva versión.
3. En la política que otorga a cualquier entidad principal el permiso para usar una plantilla de lanzamiento, restrinja la asociación de `$latest` y `$default` especificando `"autoscaling:LaunchTemplateVersionSpecified": "true"`. Al restringir el uso a una versión específica de una plantilla de lanzamiento, puede asegurarse de que las nuevas instancias se iniciarán con la versión en la que están configuradas las opciones de metadatos de la instancia. Para obtener más información, consulte LaunchTemplateSpecification en la Referencia de la API de Amazon EC2 Auto Scaling, en concreto el parámetro `Version`.
4. Para un grupo de Auto Scaling que utilice una configuración de lanzamiento, reemplace la configuración de lanzamiento por una plantilla de lanzamiento. Para obtener más información, consulte Reemplazar una configuración de lanzamiento por una plantilla de lanzamiento en la Guía del usuario de Amazon EC2 Auto Scaling.
5. Para un grupo de Auto Scaling que utilice una plantilla de lanzamiento, asegúrese de que utiliza una nueva plantilla de lanzamiento con las opciones de metadatos de la instancia configuradas o una nueva versión de la plantilla de lanzamiento actual con las opciones de metadatos de la instancia configuradas. Para obtener más información, consulte update-auto-scaling-group en la Referencia de comandos de la AWS CLI.

Ejemplos

- Requerir el uso de IMDSv2
- Denegar la exclusión voluntaria de IMDSv2
- Especificar el límite máximo de saltos
- Limitar quién puede modificar las opciones de metadatos de instancia
- Exigir que las credenciales de rol se recuperen de IMDSv2

Requerir el uso de IMDSv2

La siguiente política especifica que no se puede llamar a la API RunInstances a menos que la instancia también requiera el uso de IMDSv2 (indicado por `"ec2:MetadataHttpTokens": "required"`). Si no especifica que la instancia requiere IMDSv2, obtendrá un error `UnauthorizedOperation` cuando llame a la API RunInstances.

```
{
    "Version": "2012-10-17",
    "Statement": [
                {
            "Sid": "RequireImdsV2",
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "StringNotEquals": {
                    "ec2:MetadataHttpTokens": "required"
                }
            }
        }
    ]
}
```

Denegar la exclusión voluntaria de IMDSv2

La siguiente política especifica que no se puede llamar a la API de `ModifyInstanceMetadataOptions` y se permite la opción IMDSv1 o IMDSv2. Si llama a la API de `ModifyInstanceMetadataOptions`, el atributo `HttpTokens` debe estar establecido en `required`.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "DenyIMDSv1HttpTokensModification",
        "Effect": "Deny",
        "Action": "ec2:ModifyInstanceMetadataOptions",
        "Resource": "arn:aws:ec2:*:*:instance/*",
        "Condition": {
            "StringNotEquals": {
                "ec2:Attribute/HttpTokens": "required"
            },
```

```
            "Null": {
                "ec2:Attribute/HttpTokens": false
            }
        }
    }]
}
```

Especificar el límite máximo de saltos

La siguiente política especifica que no se puede llamar a la API RunInstances a menos que también especifique un límite de saltos y que el límite de saltos no sea superior a 3. Si no se cumplen estos requisitos, aparece un error `Unauthorized0peration` al llamar a la API RunInstances.

```
{
    "Version": "2012-10-17",
    "Statement": [
               {
            "Sid": "MaxImdsHopLimit",
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "NumericGreaterThan": {
                    "ec2:MetadataHttpPutResponseHopLimit": "3"
                }
            }
        }
    ]
}
```

Limitar quién puede modificar las opciones de metadatos de instancia

La siguiente política solo permite que los usuarios con el rol `ec2-imds-admins` hagan cambios en las opciones de metadatos de instancia. Si alguna entidad principal que no sea el rol `ec2-imds-admins` intenta llamar a la API ModifyInstanceMetadataOptions, aparecerá un error `Unauthorized0peration`. Esta instrucción podría utilizarse para controlar el uso de la API ModifyInstanceMetadataOptions; actualmente no hay controles de acceso detallados (condiciones) para la API ModifyInstanceMetadataOptions.

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
               {
            "Sid": "AllowOnlyImdsAdminsToModifySettings",
            "Effect": "Deny",
            "Action": "ec2:ModifyInstanceMetadataOptions",
            "Resource": "*",
            "Condition": {
                "StringNotLike": {
                    "aws:PrincipalARN": "arn:aws:iam::*:role/ec2-imds-admins"
                }
            }
        }
    ]
}
```

Exigir que las credenciales de rol se recuperen de IMDSv2

La siguiente política especifica que si esta política se aplica a un rol y el servicio EC2 asume el rol y las credenciales resultantes se utilizan para firmar una solicitud, la solicitud debe estar firmada por las credenciales de rol EC2 recuperadas de IMDSv2. De lo contrario, todas sus llamadas a la API obtendrán un error `Unauthorized0peration`. Esta instrucción/política se puede aplicar de manera general porque, si la solicitud no está firmada por las credenciales del rol de EC2, no tiene ningún efecto.

```
{
    "Version": "2012-10-17",
    "Statement": [
               {
            "Sid": "RequireAllEc2RolesToUseV2",
            "Effect": "Deny",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "NumericLessThan": {
                    "ec2:RoleDelivery": "2.0"
                }
            }
        }
    ]
}
```

Uso de volúmenes e instantáneas de Amazon EBS

Para obtener ejemplos de políticas para trabajar con volúmenes e instantáneas de Amazon EBS, consulte Ejemplos de políticas basadas en identidad para Amazon EBS.

Políticas de ejemplo para trabajar en la consola de Amazon EC2

Tiene que conceder a los usuarios los permisos que necesitan para Amazon EC2 mediante políticas de IAM. Puede utilizar políticas de IAM para conceder a los usuarios permisos para ver y utilizar recursos específicos en la consola de Amazon EC2. Puede utilizar las políticas de ejemplo de la sección anterior; sin embargo, estas son específicas para solicitudes que se realizan con la AWS CLI o un AWS SDK. Para obtener más información, consulte Políticas de ejemplo para trabajar con la AWS CLI o un SDK de AWS y Creación de políticas de IAM en la Guía del usuario de IAM.

La consola utiliza acciones de API adicionales para sus características, por lo que es posible que estas políticas no funcionen como es debido. Por ejemplo, un usuario que tenga permiso para utilizar únicamente la acción de API `DescribeVolumes` obtendrá errores cuando intente ver volúmenes en la consola. En esta sección se muestran políticas que permiten a los usuarios utilizar partes específicas de la consola. Para obtener más información acerca de cómo crear políticas para la consola de Amazon EC2, consulte la siguiente publicación del Blog de seguridad de AWS: Granting Users Permission to Work in the Amazon EC2 Console.

> **Tip**
>
> Para ayudarle a establecer qué acciones de API son necesarias para realizar tareas en la consola, puede utilizar un servicio como AWS CloudTrail. Para obtener más información, consulte la Guía del usuario de AWS CloudTrail. Si su política no concede permiso para crear o modificar un recurso concreto, la consola muestra un mensaje codificado con información de diagnóstico. Puede descodificar el mensaje mediante la acción DecodeAuthorizationMessage de la API para AWS STS o el comando decode-authorization-message de la AWS CLI.

Ejemplos

- Ejemplo: Acceso de solo lectura
- Ejemplo: uso del asistente de inicialización de instancias de EC2
- Ejemplo: Trabajar con grupos de seguridad
- Ejemplo: Trabajar con direcciones IP elásticas

- Ejemplo: Trabajar con Instancias reservadas

Ejemplo: Acceso de solo lectura

Para permitir a los usuarios ver todos los recursos de la consola de Amazon EC2, puede utilizar la política del ejemplo siguiente: Ejemplo: Acceso de solo lectura. Los usuarios no pueden realizar ninguna acción en dichos recursos ni crear recursos nuevos a menos que otra instrucción les conceda permiso para ello.

Ver instancias, AMI e instantáneas

Como alternativa, puede proporcionar acceso de solo lectura a un subconjunto de recursos. Para ello, reemplace el carácter comodín * en la acción de API `ec2:Describe` con acciones `ec2:Describe` específicas para cada recurso. La siguiente política permite a los usuarios ver todas las instancias, AMI e instantáneas de la consola de Amazon EC2. La acción `ec2:DescribeTags` permite a los usuarios ver AMI públicas. La consola exige la información de etiquetado para mostrar las AMI públicas; sin embargo, puede eliminar esta acción para permitir que los usuarios vean únicamente AMI privadas.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeInstances",
         "ec2:DescribeImages",
         "ec2:DescribeTags",
         "ec2:DescribeSnapshots"
      ],
      "Resource": "*"
   }
   ]
}
```

> **Note**
>
> Las acciones de API `ec2:Describe*` de Amazon EC2 no admiten los permisos de nivel de recursos, por lo que no puede controlar qué recursos individuales pueden ver los usuarios en la consola. Por lo tanto, el carácter comodín * es necesario en el elemento `Resource` de la instrucción anterior. Para obtener más información acerca de qué ARN puede usar con qué

acciones de la API de Amazon EC2, consulte Acciones, recursos y claves de condición para Amazon EC2.

Ver instancias y métricas de CloudWatch

La siguiente política permite a los usuarios ver instancias en la consola de Amazon EC2; así como alarmas y métricas de CloudWatch en la pestaña Monitorización de la página Instancia. La consola de Amazon EC2 utiliza la API de CloudWatch para visualizar las alarmas y las métricas, por lo que debe conceder a los usuarios permiso para utilizar las acciones `cloudwatch:DescribeAlarms`, `cloudwatch:DescribeAlarmsForMetric`, `cloudwatch:ListMetrics`, `cloudwatch:GetMetricStatistics` y `cloudwatch:GetMetricData`.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeInstances",
         "ec2:DescribeInstanceTypes",
         "cloudwatch:DescribeAlarms",
         "cloudwatch:DescribeAlarmsForMetric",
         "cloudwatch:ListMetrics",
         "cloudwatch:GetMetricStatistics",
         "cloudwatch:GetMetricData"
      ],
      "Resource": "*"
   }
   ]
}
```

Ejemplo: uso del asistente de inicialización de instancias de EC2

El asistente de inicialización de instancias de Amazon EC2 consiste en una pantalla con opciones para configurar y iniciar una instancia. Su política debe incluir un permiso para utilizar acciones de la API que permitan a los usuarios trabajar con opciones del asistente. Si su política no incluye dicho permiso, algunos elementos del asistente no se podrán cargar correctamente y los usuarios no podrán completar el lanzamiento.

Acceso al asistente básico de instancias de lanzamiento

Para completar correctamente un lanzamiento, debe darse a los usuarios permiso para utilizar la acción de API `ec2:RunInstances` y, como mínimo, las acciones de API siguientes:

- `ec2:DescribeImages`: ver y seleccionar una AMI.
- `ec2:DescribeInstanceTypes`: permite ver y seleccionar un tipo de instancia.
- `ec2:DescribeVpcs`: ver las opciones de red disponibles.
- `ec2:DescribeSubnets`: ver todas las subredes disponibles de la VPC elegida.
- `ec2:DescribeSecurityGroups` o `ec2:CreateSecurityGroup`: para ver y seleccionar un grupo de seguridad existente o para crear uno nuevo.
- `ec2:DescribeKeyPairs` o `ec2:CreateKeyPair`: seleccionar un par de claves existente o para crear uno nuevo.
- `ec2:AuthorizeSecurityGroupIngress`: añadir reglas de entrada.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeImages",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "ec2:CreateSecurityGroup",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateKeyPair"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "*"
        }
    ]
}
```

Puede añadir acciones de API a su política para proporcionar más opciones para los usuarios; por ejemplo:

- `ec2:DescribeAvailabilityZones`: ver y seleccionar una zona de disponibilidad específica.
- `ec2:DescribeNetworkInterfaces`: ver y seleccionar interfaces de red existentes para la subred seleccionada.
- Para añadir reglas de salida a grupos de seguridad de VPC, debe conceder permiso a los usuarios para utilizar la acción de API `ec2:AuthorizeSecurityGroupEgress`. Para modificar o eliminar reglas ya existentes, debe conceder permiso a los usuarios para utilizar la acción de API `ec2:RevokeSecurityGroup*` pertinente.
- `ec2:CreateTags`: etiquetar los recursos que `RunInstances` crea. Para obtener más información, consulte Conceder permisos para etiquetar recursos durante la creación. Si los usuarios no tienen permiso para utilizar esta acción e intentan aplicar etiquetas en la página de etiquetado del asistente para el lanzamiento de instancias, el lanzamiento generará un error.

  > **Important**
  >
  > Especificar un valor en Nombre al iniciar una instancia crea una etiqueta y requiere la acción `ec2:CreateTags`. Tenga cuidado al conceder a los usuarios permiso para usar la acción `ec2:CreateTags`, ya que ello limita su capacidad de usar la clave de condición `aws:ResourceTag` para restringir el uso de otros recursos. Si concede permiso a los usuarios para usar la acción `ec2:CreateTags`, pueden cambiar la etiqueta de un recurso para omitir esas restricciones. Para obtener más información, consulte Control del acceso a recursos de EC2 mediante etiquetas de recursos.

- Para utilizar parámetros de Systems Manager al seleccionar una AMI, debe agregar `ssm:DescribeParameters` y `ssm:GetParameters` a la política. `ssm:DescribeParameters` concede a los usuarios el permiso para ver y seleccionar parámetros de Systems Manager. `ssm:GetParameters` concede a los usuarios el permiso para obtener los valores de los parámetros de Systems Manager. También puede restringir el acceso a parámetros de Systems Manager específicos. Para obtener más información, vea Restringir el acceso a parámetros específicos de Administrador de sistemas más adelante en esta sección.

Actualmente, las acciones `Describe*` de la API de Amazon EC2 no admiten los permisos de nivel de recursos, por lo que no puede restringir qué recursos individuales pueden ver los usuarios en el asistente para el lanzamiento de instancias. Sin embargo, puede aplicar permisos de nivel de

recursos en la acción de API `ec2:RunInstances` para restringir qué recursos pueden utilizar los usuarios para iniciar una instancia. El lanzamiento generará un error si los usuarios seleccionan opciones sobre las que no tienen permiso de uso.

Limitar el acceso a un tipo de instancia, subred y región específicos

La política siguiente permite a los usuarios iniciar instancias `t2.micro` utilizando AMI propiedad de Amazon y únicamente en una subred concreta (`subnet-1a2b3c4d`). Los usuarios solo pueden realizar lanzamientos en la región `sa-east-1`. Si seleccionan otra región u otro tipo de instancia, AMI o subred en el asistente para el lanzamiento de instancias, el lanzamiento generará un error.

La primera instrucción concede a los usuarios permiso para ver las opciones del asistente para el lanzamiento de instancias, tal y como se demuestra en el ejemplo anterior. La segunda instrucción concede a los usuarios permiso para utilizar recursos de la interfaz de red, el volumen, el par de claves, el grupo de seguridad y la subred para la acción `ec2:RunInstances`, necesarios para iniciar una instancia en una VPC. Para obtener información sobre cómo usar la acción `ec2:RunInstances`, consulte Iniciar instancias (RunInstances). La tercera y la cuarta instrucción conceden a los usuarios permiso para utilizar la instancia y los recursos de la AMI respectivamente, pero solo si la instancia es una instancia `t2.micro` y solo si la AMI es propiedad de Amazon o de determinados socios verificados y de confianza.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeInstances",
         "ec2:DescribeImages",
         "ec2:DescribeInstanceTypes",
         "ec2:DescribeKeyPairs",
         "ec2:CreateKeyPair",
         "ec2:DescribeVpcs",
         "ec2:DescribeSubnets",
         "ec2:DescribeSecurityGroups",
         "ec2:CreateSecurityGroup",
         "ec2:AuthorizeSecurityGroupIngress"
   ],
   "Resource": "*"
   },
   {
      "Effect": "Allow",
```

```
      "Action":"ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:sa-east-1:111122223333:network-interface/*",
         "arn:aws:ec2:sa-east-1:111122223333:volume/*",
         "arn:aws:ec2:sa-east-1:111122223333:key-pair/*",
         "arn:aws:ec2:sa-east-1:111122223333:security-group/*",
         "arn:aws:ec2:sa-east-1:111122223333:subnet/subnet-1a2b3c4d"
      ]
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:sa-east-1:111122223333:instance/*"
      ],
      "Condition": {
         "StringEquals": {
            "ec2:InstanceType": "t2.micro"
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
           "arn:aws:ec2:sa-east-1::image/ami-*"
      ],
      "Condition": {
         "StringEquals": {
            "ec2:Owner": "amazon"
         }
      }
   }
   ]
}
```

Restringir el acceso a parámetros específicos de Administrador de sistemas

La siguiente política concede acceso para utilizar parámetros de Systems Manager con un nombre específico.

La primera instrucción concede a los usuarios permiso para ver parámetros de Systems Manager al seleccionar una AMI en el asistente de lanzamiento de instancias. La segunda instrucción concede a los usuarios el permiso para utilizar solo parámetros con nombre `prod-*`.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ssm:DescribeParameters"
      ],
      "Resource": "*"
   },
   {
      "Effect": "Allow",
      "Action": [
         "ssm:GetParameters"
      ],
     "Resource": "arn:aws:ssm:us-east-2:123456123:parameter/prod-*"
   }
   ]
}
```

Ejemplo: Trabajar con grupos de seguridad

Ver los grupos de seguridad y añadir y eliminar reglas

La siguiente política concede a los usuarios permiso para ver grupos de seguridad en la consola de Amazon EC2, así como para agregar y quitar reglas de entrada y salida y enumerar y modificar las descripciones de las reglas de los grupos de seguridad existentes que tengan la etiqueta `Department=Test`.

En la primera instrucción, la acción `ec2:DescribeTags` permite a los usuarios ver etiquetas en la consola, lo que les facilita la identificación de los grupos de seguridad sobre los que tienen permiso de modificación.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeSecurityGroups",
```

```
            "ec2:DescribeSecurityGroupRules",
            "ec2:DescribeTags"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:AuthorizeSecurityGroupIngress",
            "ec2:RevokeSecurityGroupIngress",
            "ec2:AuthorizeSecurityGroupEgress",
            "ec2:RevokeSecurityGroupEgress",
            "ec2:ModifySecurityGroupRules",
            "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
            "ec2:UpdateSecurityGroupRuleDescriptionsEgress"
        ],
        "Resource": [
            "arn:aws:ec2:region:111122223333:security-group/*"
        ],
        "Condition": {
            "StringEquals": {
                "aws:ResourceTag/Department": "Test"
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:ModifySecurityGroupRules"
        ],
        "Resource": [
            "arn:aws:ec2:region:111122223333:security-group-rule/*"
        ]
    }
]}
```

Trabajar con el cuadro de diálogo Crear grupo de seguridad

Puede crear una política que permita a los usuarios trabajar con el cuadro de diálogo Crear grupo de seguridad en la consola de Amazon EC2. Para utilizar este cuadro de diálogo, debe darse a los usuarios permiso para utilizar como mínimo las acciones de API siguientes:

- `ec2:CreateSecurityGroup`: crear un nuevo grupo de seguridad.

- `ec2:DescribeVpcs`: ver una lista de las VPC existentes en la lista VPC.

Con estos permisos, los usuarios pueden crear correctamente un grupo de seguridad nuevo, pero no pueden añadirle reglas. Para trabajar con reglas en el cuadro de diálogo Crear grupo de seguridad, puede añadir las acciones de la API siguientes a una política:

- `ec2:AuthorizeSecurityGroupIngress`: añadir reglas de entrada.
- `ec2:AuthorizeSecurityGroupEgress`: añadir reglas de salida a grupos de seguridad de la VPC.
- `ec2:RevokeSecurityGroupIngress`: modificar o eliminar reglas de entradas existentes. Esta acción es útil para permitir a los usuarios utilizar la característica Copiar en uno nuevo de la consola. La característica abre el cuadro de diálogo Crear grupo de seguridad y lo rellena con las mismas reglas que el grupo de seguridad que se seleccionó.
- `ec2:RevokeSecurityGroupEgress`: modificar o eliminar reglas de salida de grupos de seguridad de la VPC. Es útil para permitir a los usuarios modificar o eliminar la regla de salida predeterminada que permite todo el tráfico de salida.
- `ec2:DeleteSecurityGroup`: responder cuando las reglas no válidas no se pueden guardar. La consola crea primero el grupo de seguridad y después añade las reglas especificadas. Si las reglas no son válidas, la acción genera un error y la consola intenta eliminar el grupo de seguridad. El usuario permanece en el cuadro de diálogo Crear grupo de seguridad para que se pueda corregir la regla no válida y volver a intentar crear el grupo de seguridad. Esta acción de API no es obligatoria, pero si no se concede a un usuario permiso para utilizarla y el usuario intenta crear un grupo de seguridad con reglas no válidas, el grupo de seguridad se creará sin reglas y el usuario deberá añadirlas después.
- `ec2:UpdateSecurityGroupRuleDescriptionsIngress`: para agregar o actualizar descripciones de reglas de grupo de seguridad de entrada (entrantes).
- `ec2:UpdateSecurityGroupRuleDescriptionsEgress`: para agregar o actualizar descripciones de reglas de grupo de seguridad de salida (salientes).
- `ec2:ModifySecurityGroupRules`: para modificar reglas de grupo de seguridad.
- `ec2:DescribeSecurityGroupRules`: para enumerar reglas de grupo de seguridad.

La siguiente política concede a los usuarios permiso para utilizar el cuadro de diálogo Crear grupo de seguridad y para crear reglas de entrada y de salida para los grupos de seguridad que están asociados a una VPC específica (`vpc-1a2b3c4d`). Los usuarios pueden crear grupos de seguridad

para una VPC, pero no pueden agregarles reglas. Igualmente, los usuarios tampoco pueden añadir reglas a ningún grupo de seguridad que no esté asociado a la VPC `vpc-1a2b3c4d`. También se concede permiso a los usuarios para ver todos los grupos de seguridad de la consola. Esto facilita a los usuarios la identificación de los grupos de seguridad a los que pueden añadir reglas de entrada. Esta política también concede a los usuarios permiso para eliminar grupos de seguridad que estén asociados a la VPC `vpc-1a2b3c4d`.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeSecurityGroups",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeVpcs"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource": "arn:aws:ec2:region:111122223333:security-group/*",
      "Condition":{
         "ArnEquals": {
            "ec2:Vpc": "arn:aws:ec2:region:111122223333:vpc/vpc-1a2b3c4d"
         }
      }
    }
   ]
}
```

Ejemplo: Trabajar con direcciones IP elásticas

Para permitir a los usuarios ver direcciones IP elásticas en la consola de Amazon EC2, debe concederles permiso para utilizar la acción `ec2:DescribeAddresses`.

Para permitir a los usuarios trabajar con direcciones IP elásticas, puede añadir las siguientes acciones a su política.

- `ec2:AllocateAddress`: asignar una dirección IP elástica.
- `ec2:ReleaseAddress`: liberar una dirección IP elástica.
- `ec2:AssociateAddress`: asociar una dirección IP elástica a una instancia o una interfaz de red.
- `ec2:DescribeNetworkInterfaces` y `ec2:DescribeInstances`: trabajar con la pantalla Asociar dirección. La pantalla muestra las instancias o las interfaces de red disponibles a las que se puede adjuntar una dirección IP elástica.
- `ec2:DisassociateAddress`: desvincular una dirección IP elástica de una instancia o una interfaz de red.

La siguiente política permite a los usuarios ver, asignar y asociar direcciones IP elásticas a instancias. Los usuarios no pueden asociar direcciones IP elásticas a interfaces de red, desvincular direcciones IP elásticas ni liberarlas.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeAddresses",
                "ec2:AllocateAddress",
                "ec2:DescribeInstances",
                "ec2:AssociateAddress"
            ],
            "Resource": "*"
        }
    ]
}
```

Ejemplo: Trabajar con Instancias reservadas

La siguiente política permite a los usuarios ver y modificar las instancias reservadas de su cuenta, así como adquirir nuevas instancias reservadas en la AWS Management Console.

Esta política permite a los usuarios ver todas las Instancias reservadas, así como las Instancias bajo demanda, en la cuenta. No se pueden establecer permisos de nivel de recursos para Instancias reservadas individuales.

```
{
```

```
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeReservedInstances",
         "ec2:ModifyReservedInstances",
         "ec2:PurchaseReservedInstancesOffering",
         "ec2:DescribeInstances",
         "ec2:DescribeInstanceTypes",
         "ec2:DescribeAvailabilityZones",
         "ec2:DescribeReservedInstancesOfferings"
      ],
      "Resource": "*"
   }
   ]
}
```

La acción `ec2:DescribeAvailabilityZones` es necesaria para garantizar que la consola de Amazon EC2 pueda mostrar información sobre las zonas de disponibilidad en las que se pueden adquirir Instancias reservadas. La acción `ec2:DescribeInstances` no es obligatoria, pero permite asegurarse de que el usuario pueda ver las instancias de la cuenta y adquirir reservas para correlacionar las especificaciones correctas.

Puede ajustar las acciones de API para limitar el acceso de los usuarios; por ejemplo, si quita `ec2:DescribeInstances` y `ec2:DescribeAvailabilityZones`, el usuario tendrá acceso de solo lectura.

Políticas administradas de AWS para Amazon EC2

Para agregar permisos a usuarios, grupos y roles, es más fácil utilizar las políticas administradas de AWS que escribirlas uno mismo. Se necesita tiempo y experiencia para crear políticas administradas por el cliente de IAM que le brinden a su equipo solo los permisos necesarios. Para comenzar a hacerlo con rapidez, puede utilizar nuestras políticas administradas de AWS. Estas políticas cubren casos de uso comunes y están disponibles en su cuenta de AWS. Para obtener más información sobre las políticas administradas por AWS, consulte Políticas administradas por AWS en la Guía del usuario de IAM.

Los servicios de AWS mantienen y actualizan las políticas administradas por AWS. No puede cambiar los permisos en las políticas administradas de AWS. En ocasiones, los servicios agregan permisos adicionales a una política administrada por AWS para admitir características nuevas. Este

tipo de actualización afecta a todas las identidades (usuarios, grupos y roles) donde se asocia la política. Es más probable que los servicios actualicen una política administrada por AWScuando se lanza una nueva característica o cuando se ponen a disposición nuevas operaciones. Los servicios no quitan los permisos de una política administrada de AWS, por lo tanto, las actualizaciones de las políticas no deteriorarán los permisos existentes.

Además, AWS admite políticas administradas para funciones de trabajo que abarcan varios servicios. Por ejemplo, la política administrada de AWS ReadOnlyAccess proporciona acceso de solo lectura a todos los servicios y los recursos de AWS. Cuando un servicio lanza una nueva característica, AWS agrega permisos de solo lectura para las operaciones y los recursos nuevos. Para obtener una lista y descripciones de las políticas de funciones de trabajo, consulte Políticas administradas de AWS para funciones de trabajo en la Guía del usuario de IAM.

Política administrada de AWS: AmazonEC2FullAccess

Puede adjuntar la política `AmazonEC2FullAccess` a las identidades de IAM. Esta política otorga permisos que permiten el acceso completo a Amazon EC2.

Para ver los permisos de esta política, consulte AmazonEC2FullAccess en la Referencia de la política administrada de AWS.

Política administrada de AWS: AmazonEC2ReadOnlyAccess

Puede adjuntar la política `AmazonEC2ReadOnlyAccess` a las identidades de IAM. Esta política otorga permisos que brindan acceso de solo lectura a Amazon EC2.

Para ver los permisos de esta política, consulte AmazonEC2ReadOnlyAccess en la Referencia de la política administrada de AWS.

Política administrada de AWS: AWSEC2CapacityReservationFleetRolePolicy

Esta política está asociada al rol vinculado a un servicio denominado AWSServiceRoleForEC2CapacityReservationFleet para permitir que las reservas de capacidad creen, modifiquen y cancelen reservas de capacidad en su nombre. Para obtener más información, consulte Rol vinculado al servicio para la flota de reservas de capacidad.

Para ver los permisos de esta política, consulte AWSEC2CapacityReservationFleetRolePolicy en la Referencia de la política administrada de AWS.

Política administrada AWS: AWSEC2FleetServiceRolePolicy

Esta política se adjunta al rol vinculado a un servicio denominado AWSServiceRoleForEC2Fleet para permitir que la flota de EC2 solicite, lance, termine y etiquete instancias en su nombre. Para obtener más información, consulte Rol vinculado al servicio de flota de EC2.

Para ver los permisos de esta política, consulte AWSEC2FleetServiceRolePolicy en la Referencia de la política administrada de AWS.

Política administrada AWS: AWSEC2SpotFleetServiceRolePolicy

Esta política se adjunta al rol vinculado a un servicio denominado AWSServiceRoleForEC2SpotFleet para permitir que la flota de spot lance y administre instancias en su nombre. Para obtener más información, consulte Rol vinculado a servicios de flota de spot.

Para ver los permisos de esta política, consulte AWSEC2SpotFleetServiceRolePolicy en la Referencia de la política administrada de AWS.

Política administrada AWS: AWSEC2SpotServiceRolePolicy

Esta política se adjunta al rol vinculado a un servicio denominado AWSServiceRoleForEC2Spot para permitir que Amazon EC2 lance y administre instancias de spot en su nombre. Para obtener más información, consulte Rol vinculado al servicio para solicitudes de instancias de spot.

Para ver los permisos de esta política, consulte AWSEC2SpotServiceRolePolicy en la Referencia de la política administrada de AWS.

Política administrada de AWS: AWSEC2VssSnapshotPolicy

Puede adjuntar esta política administrada al rol de perfil de instancia de IAM que utiliza para sus instancias Windows de Amazon EC2. La política concede permisos que permiten a Amazon EC2 crear y administrar instantáneas de VSS en su nombre.

Para ver los permisos de esta política, consulte AWSEC2VssSnapshotPolicy en la Referencia de la política administrada de AWS.

Política administrada AWS: EC2FastLaunchFullAccess

Puede asociar la política `EC2FastLaunchFullAccess` al perfil de instancia u otro rol de IAM. Esta política otorga acceso total a las acciones del lanzamiento rápido de EC2 y a los permisos específicos que se indican a continuación.

Detalles de los permisos

- Lanzamiento rápido de EC2: se concede el acceso administrativo para que el rol pueda activar o desactivar el lanzamiento rápido de EC2 y describir las imágenes de lanzamiento rápido de EC2.
- Amazon EC2: se concede acceso a las acciones RunInstances, CreateTags y Describe de Amazon EC2 necesarias para verificar los permisos de los recursos.
- IAM: se concede acceso para obtener y utilizar los perfiles de instancia cuyos nombres contengan `ec2fastlaunch` para crear el rol vinculado a un servicio EC2FastLaunchServiceRolePolicy.

Para ver los permisos de esta política, consulte EC2FastLaunchFullAccess en la Referencia de la política administrada de AWS.

Política administrada AWS: EC2FastLaunchServiceRolePolicy

Esta política está asociada al rol vinculado a un servicio denominado AWSServiceRoleForEC2FastLaunch para permitir que Amazon EC2 cree y administre un conjunto de instantáneas aprovisionadas previamente que reducen el tiempo que tarda en lanzar instancias desde la AMI con el lanzamiento rápido de EC2 habilitado. Para obtener más información, consulte the section called “Rol vinculado al servicio”.

Para ver los permisos de esta política, consulte EC2FastLaunchServiceRolePolicy en la Referencia de la política administrada de AWS.

Política administrada de AWS: Ec2InstanceConnectEndpoint

Esta política se asocia al rol vinculado a un servicio denominado AWSServiceRoleForEC2InstanceConnect para permitir que el punto de conexión de EC2 Instance Connect realice acciones en su nombre. Para obtener más información, consulte Rol vinculado a un servicio del punto de conexión de EC2 Instance Connect.

Para ver los permisos de esta política, consulte Ec2InstanceConnectEndpoint en la Referencia de la política administrada de AWS.

Actualizaciones de Amazon EC2 en las políticas administradas por AWS

Es posible consultar los detalles sobre las actualizaciones de las políticas administradas por AWS para Amazon EC2 debido a que este servicio comenzó a realizar el seguimiento de estos cambios.

Cambio	Descripción	Fecha
EC2FastLaunchFullAccess: política nueva	Amazon EC2 agregó la política para realizar acciones de API relacionadas con la característica de lanzamien to rápido de EC2 desde una instancia. La política se puede adjuntar al perfil de instancia de una instancia que se lance desde una AMI con el lanzamiento rápido de EC2 habilitado.	14 de mayo de 2024
AWSEC2VssSnapshotPolicy: política nueva	Amazon EC2 agregó la política `AWSEC2Vss SnapshotPolicy` que contiene los permisos para crear y añadir etiquetas a las instantáneas de Amazon Machine Images (AMI) y de EBS.	28 de marzo de 2024
EC2FastLaunchServi ceRolePolicy: política nueva	Amazon EC2 agregó la característica de lanzamiento rápido de EC2 para permitir que las AMI de Windows lancen instancias más rápido con la creación de un conjunto de instantáneas aprovisio nadas previamente.	26 de noviembre de 2021
Amazon EC2 comenzó a realizar el seguimiento de los cambios	Amazon EC2 comenzó a realizar el seguimiento de los cambios en sus políticas administradas de AWS	1 de marzo de 2021

Roles de IAM para Amazon EC2

Las aplicaciones deben firmar sus solicitudes de API con credenciales de AWS. Por lo tanto, si es usted un desarrollador de aplicaciones, necesitará una estrategia para administrar las credenciales de sus aplicaciones que se ejecuten en instancias de EC2. Por ejemplo, puede distribuir con seguridad sus credenciales de AWS a las instancias, lo que habilita las aplicaciones que tiene en dichas instancias para que utilicen sus credenciales a fin de firmar solicitudes y, al mismo tiempo, proteger sus credenciales respecto a otros usuarios. Sin embargo, distribuir las credenciales a cada instancia de forma segura plantea ciertas dificultades, en especial cuando se trata de aquellas que AWS crea en su nombre, como las instancias de spot o las de los grupos de Auto Scaling. También debe poder actualizar las credenciales de cada instancia cuando rota sus credenciales de AWS.

> **Note**
>
> Para sus cargas de trabajo de Amazon EC2, le recomendamos que recupere las credenciales de sesión mediante el método que se describe a continuación. Estas credenciales deberían permitir a su carga de trabajo realizar solicitudes de API de AWS, sin necesidad de usar `sts:AssumeRole` para asumir el mismo rol que ya está asociado a la instancia. A menos que necesite pasar etiquetas de sesión para el control de acceso basado en atributos (ABAC) o pasar una política de sesión para restringir aún más los permisos del rol, estas llamadas de asunción de roles no son necesarias, ya que crean un nuevo conjunto de las mismas credenciales temporales de sesión de rol.
> Si su carga de trabajo usa un rol para asumirse a sí mismo, debe crear una política de confianza que permita explícitamente que ese rol se asuma a sí mismo. Si no crea la política de confianza, obtiene el error `AccessDenied`. Para obtener más información, consulte Modificación de una política de confianza de rol en la Guía del usuario de IAM.

Hemos diseñado los roles de IAM, para que sus aplicaciones puedan realizar solicitudes de API con seguridad desde sus instancias, sin que usted tenga que administrar las credenciales de seguridad que la aplicación utiliza. En lugar de crear y distribuir sus credenciales de AWS, puede delegar el permiso para realizar solicitudes de API mediante los roles de IAM, tal como se indica a continuación:

1. Cree de un rol de IAM.
2. Defina qué cuentas o servicios de AWS pueden asumir el rol.
3. Defina qué acciones y recursos de la API puede utilizar la aplicación después de asumir el rol.
4. Especifique el rol cuando lance su instancia, o asocie el rol a una instancia existente.

5. Haga que la aplicación recupere unas credenciales temporales y las use.

Por ejemplo, puede utilizar roles de IAM para conceder permisos a aplicaciones que se ejecutan en sus instancias y que necesitan utilizar un bucket en Amazon S3. Puede especificar permisos para roles de IAM, creando una política en formato JSON. Son parecidos a las políticas que crea para usuarios de . Si cambia un rol, el cambio se propaga a todas las instancias.

> **Note**
>
> Las credenciales del rol de IAM de Amazon EC2 no están sujetas a la duración máxima de sesión configurada en el rol. Para obtener más información, consulte Uso de roles de IAM en la guía del usuario de IAM.

Al crear roles de IAM, asocie las políticas de IAM con privilegios mínimos que restringen el acceso a las llamadas a la API específicas que requiere la aplicación. Para la comunicación de Windows a Windows, use grupos y roles de Windows bien definidos y bien documentados para conceder acceso a nivel de aplicación entre instancias de Windows. Los grupos y roles permiten que los clientes definan permisos de nivel de carpeta NTFS y aplicaciones con privilegios mínimos para limitar el acceso a los requisitos específicos de la aplicación.

Solo puede adjuntar un rol de IAM a una instancia, pero puede adjuntar el mismo rol a muchas instancias. Para obtener más información sobre la creación y el uso de roles de IAM, consulte Roles en la Guía del usuario de IAM.

Puede aplicar permisos de nivel de recursos a sus políticas de IAM para controlar la capacidad de los usuarios de asociar, sustituir o desasociar roles de IAM de una instancia. Para obtener más información, consulte Permisos de nivel de recurso admitidos para las acciones de la API de Amazon EC2 y el siguiente ejemplo: Ejemplo: Trabajar con roles de IAM.

Contenido

Perfiles de instancias

Amazon EC2 utiliza un perfil de instancia como contenedor de un rol de IAM. Cuando se crea un rol de IAM utilizando la consola de IAM, esta crea automáticamente un perfil de instancia y le da el mismo nombre que el rol al que corresponde. Si utiliza la consola de Amazon EC2 para iniciar una instancia con un rol de IAM o para asociar un rol de IAM a una instancia, elija el rol en función de una lista de nombres de perfiles de instancias.

Si utiliza la AWS CLI, la API o un SDK de AWS para crear un rol, cree el rol y el perfil de instancia de forma independiente, con nombres potencialmente diferentes. Si posteriormente usa la AWS CLI, la API o un AWS SDK para iniciar una instancia con un rol de IAM o para adjuntar un rol de IAM a una instancia, especifique el nombre del perfil de instancias.

Un perfil de instancia solo puede contener un rol de IAM. Este límite no se puede aumentar.

Para obtener más información, consulte Instance Profiles en la Guía del usuario de IAM.

Recuperar credenciales de seguridad de los metadatos de la instancia

Una aplicación de una instancia recupera las credenciales de seguridad que proporciona el rol en el elemento `iam/security-credentials/`role-name de los metadatos de la instancia. Se conceden a la aplicación los permisos para las acciones y los recursos que usted ha definido para el rol mediante las credenciales de seguridad asociadas al rol. Estas credenciales de seguridad son temporales y las rotamos automáticamente. Activamos la disponibilidad de las nuevas credenciales al menos cinco minutos antes del vencimiento de las antiguas.

> **Warning**
>
> Si utiliza servicios que utilizan metadatos de las instancias con los roles de IAM, asegúrese de que no revela sus credenciales cuando los servicios realizan llamadas HTTP en su nombre. Los tipos de servicios que pueden llegar a revelar sus credenciales son, entre otros, proxies HTTP, servicios de validador HTML/CSS y procesadores XML que admiten la inclusión de XML.

El comando siguiente recupera las credenciales de seguridad de un rol IAM de `s3access` denominado .

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/iam/security-credentials/s3access
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/iam/security-credentials/s3access
```

Windows

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/iam/security-credentials/s3access
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/iam/security-credentials/s3access
```

A continuación, se muestra un ejemplo del resultado.

```
{
  "Code" : "Success",
  "LastUpdated" : "2012-04-26T16:39:16Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIAIOSFODNN7EXAMPLE",
  "SecretAccessKey" : "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY",
  "Token" : "token",
  "Expiration" : "2017-05-17T15:09:54Z"
```

```
}
```

Para las aplicaciones, la AWS CLI y los comandos de las herramientas para Windows PowerShell que se ejecutan en la instancia, no es necesario obtener de forma explícita las credenciales de seguridad temporales, dado que los AWS SDK, la AWS CLI y las herramientas para Windows PowerShell obtienen automáticamente las credenciales del servicio de metadatos de la instancia de EC2 y las utilizan. Para llamar fuera de la instancia utilizando credenciales de seguridad temporales (por ejemplo, para probar políticas de IAM), debe proporcionar la clave de acceso, la clave secreta y el token de la sesión. Para obtener más información, consulte Uso de credenciales de seguridad temporales para solicitar acceso a los recursos de AWS en la Guía del usuario de IAM.

Para obtener más información acerca de los metadatos de instancias, consulte Trabajar con metadatos de instancias. Para obtener información sobre la dirección IP de metadatos de instancia, consulte Recuperar metadatos de instancia.

Concesión de permisos a un usuario para transferir un rol de IAM a una instancia

Para permitir que un usuario lance una instancia con un rol de IAM o asocie o sustituya un rol de IAM a una instancia existente, debe concederle permiso para utilizar las siguientes acciones de API:

- `iam:PassRole`
- `ec2:AssociateIamInstanceProfile`
- `ec2:ReplaceIamInstanceProfileAssociation`

Por ejemplo, la siguiente política de IAM concede a los usuarios permiso para iniciar instancias con un rol de IAM, o para sustituir o adjuntar un rol de IAM para una instancia existente con la AWS CLI.

> **Note**
>
> Si quiere que la política conceda a los usuarios acceso a todos los roles, especifique el recurso como * en la política. No obstante, tenga en cuenta el principio de privilegios mínimos como práctica recomendada.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances",
         "ec2:AssociateIamInstanceProfile",
         "ec2:ReplaceIamInstanceProfileAssociation"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::123456789012:role/DevTeam*"
    }
  ]
}
```

Para conceder a los usuarios permiso para iniciar instancias con un rol de IAM o para sustituir o asociar un rol de IAM a una instancia ya existente con la consola de Amazon EC2, debe concederles permiso para utilizar `iam:ListInstanceProfiles`, `iam:PassRole`, `ec2:AssociateIamInstanceProfile` y `ec2:ReplaceIamInstanceProfileAssociation`, además de cualquier otro permiso que puedan necesitar. Para ver ejemplos de políticas, consulte Políticas de ejemplo para trabajar en la consola de Amazon EC2.

Trabajar con roles de IAM

Puede crear un rol de IAM y adjuntarlo a una instancia durante el lanzamiento o después. También puede separar o reemplazar un rol de IAM de una instancia.

Contenido

Crear un rol de IAM

Debe crear un rol de IAM antes de iniciar una instancia con dicho rol o adjuntarla a una instancia.

Console

Para crear un rol IAM con la consola de IAM

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, elija Roles y, a continuación, Crear rol.
3. En la página Seleccionar entidad de confianza, elija Servicio de AWS y, a continuación, seleccione el caso de uso de EC2. Elija Siguiente.
4. En la página Agregar permisos, seleccione las políticas que conceden a sus instancias acceso a los recursos que necesiten. Elija Siguiente.
5. En la página Asignar nombre, revisar y crear, ingrese un nombre y una descripción para el nuevo rol. De manera opcional, agregue etiquetas al rol. Elija Crear rol.

Command line

En el ejemplo siguiente se crea un rol de IAM con una política que permite que el rol utilice un bucket de Amazon S3.

Para crear un rol de IAM y un perfil de instancias (AWS CLI)

1. Cree la siguiente política de confianza y guárdela en un archivo de texto denominado `ec2-role-trust-policy.json`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": { "Service": "ec2.amazonaws.com"},
      "Action": "sts:AssumeRole"
    }
  ]
}
```

2. Cree el rol `s3access` y especifique la política de confianza que creó mediante el comando create-role.

```
aws iam create-role \
    --role-name s3access \
```

```
    --assume-role-policy-document file://ec2-role-trust-policy.json
```

Ejemplo de respuesta

```
{
    "Role": {
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Action": "sts:AssumeRole",
                    "Effect": "Allow",
                    "Principal": {
                        "Service": "ec2.amazonaws.com"
                    }
                }
            ]
        },
        "RoleId": "AROAIIZKPBKS2LEXAMPLE",
        "CreateDate": "2013-12-12T23:46:37.247Z",
        "RoleName": "s3access",
        "Path": "/",
        "Arn": "arn:aws:iam::123456789012:role/s3access"
    }
}
```

3. Cree una política de acceso y guárdela en un archivo de texto denominado `ec2-role-access-policy.json`. Por ejemplo, esta política concede permisos administrativos para Amazon S3 a aplicaciones que se ejecutan en la instancia.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:*"],
      "Resource": ["*"]
    }
  ]
}
```

4. Asocie la política de acceso al rol mediante el comando put-role-policy.

```
aws iam put-role-policy \
    --role-name s3access \
    --policy-name S3-Permissions \
    --policy-document file://ec2-role-access-policy.json
```

5. Cree un perfil de instancia denominado `s3access-profile` mediante el comando create-instance-profile.

```
aws iam create-instance-profile --instance-profile-name s3access-profile
```

Ejemplo de respuesta

```
{
    "InstanceProfile": {
        "InstanceProfileId": "AIPAJTLBPJLEGREXAMPLE",
        "Roles": [],
        "CreateDate": "2013-12-12T23:53:34.093Z",
        "InstanceProfileName": "s3access-profile",
        "Path": "/",
        "Arn": "arn:aws:iam::123456789012:instance-profile/s3access-profile"
    }
}
```

6. Añada el rol `s3access` al perfil de instancia `s3access-profile`.

```
aws iam add-role-to-instance-profile \
    --instance-profile-name s3access-profile \
    --role-name s3access
```

También puede usar los siguientes comandos de AWS Tools for Windows PowerShell:

- New-IAMRole
- Register-IAMRolePolicy
- New-IAMInstanceProfile

Iniciar una instancia con un rol de IAM

Después de crear un rol de IAM, puede iniciar una instancia y asociar dicho rol a la instancia durante el lanzamiento.

> **Important**
>
> Después de crear un rol de IAM, los permisos pueden tardar unos segundos en propagarse. Si su primer intento de iniciar una instancia con un rol da un error, espere unos cuantos segundos antes de volverlo a intentar. Para obtener más información, consulte Solución de problemas de roles de IAM en la Guía del usuario de IAM.

New console

Para lanzar una instancia con un rol de IAM (consola)

1. Siga el procedimiento para lanzar una instancia.
2. Expanda Detalles avanzados y en Perfil de instancia de IAM, seleccione el rol de IAM que creó.

   > **Note**
   >
   > La lista Perfil de instancia de IAM muestra el nombre del perfil de instancia que creó al crear el rol de IAM. Si creó su rol de IAM con la consola, el perfil de instancia se creó en su nombre y se le dio el mismo nombre que el rol. Si creó el rol de IAM con la AWS CLI, la API o un AWS SDK, es posible que le haya dado un nombre distinto a su perfil de instancias.

3. Configure cualquier otro detalle que necesite para la instancia o acepte los valores predeterminados y, luego, seleccione un par de claves. Para obtener información acerca de los campos del asistente de lanzamiento de instancias, consulte iniciar una instancia mediante parámetros definidos.
4. En el panel Summary (Resumen), revise la configuración de la instancia y, a continuación, elija Launch instance (Lanzar instancia).
5. Si utiliza las acciones de la API de Amazon EC2 en su aplicación, recupere las credenciales de seguridad de AWS que están disponibles en la instancia y úselas para firmar las solicitudes. El SDK de AWS se encarga de ello por usted.

IMDSv2

Para instancias de Linux, consulte el siguiente ejemplo:

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
 "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
meta-data/iam/security-credentials/role_name
```

Para instancias de Windows, consulte el siguiente ejemplo:

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-
ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token}
 -Method GET -Uri http://169.254.169.254/latest/meta-data/iam/security-
credentials/role_name
```

IMDSv1

Para instancias de Linux, consulte el siguiente ejemplo:

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/iam/security-
credentials/role_name
```

Para instancias de Windows, consulte el siguiente ejemplo:

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/iam/
security-credentials/role_name
```

Old console

Para lanzar una instancia con un rol de IAM (consola)

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel, elija Iniciar instancia.

3. Seleccione una AMI y un tipo de instancia y, a continuación, elija Siguiente: Configurar detalles de instancia.
4. En la página Configurar detalles de instancia, en Rol de IAM, seleccione el rol de IAM que ha creado.

   > **Note**
   >
   > La lista Rol de IAM muestra el nombre del perfil de instancia que creó al crear el rol de IAM. Si creó su rol de IAM con la consola, el perfil de instancia se creó en su nombre y se le dio el mismo nombre que el rol. Si creó el rol de IAM con la AWS CLI, la API o un AWS SDK, es posible que le haya dado un nombre distinto a su perfil de instancias.

5. Configure todos los demás detalles y, a continuación, siga las instrucciones del resto del asistente o elija Revisar e iniciar) para aceptar la configuración predeterminada e ir directamente a la página Revisar lanzamiento de instancia.
6. Revise la configuración y, a continuación, elija Iniciar para seleccionar un par de claves y iniciar la instancia.
7. Si utiliza las acciones de la API de Amazon EC2 en su aplicación, recupere las credenciales de seguridad de AWS que están disponibles en la instancia y úselas para firmar las solicitudes. El SDK de AWS se encarga de ello por usted.

   IMDSv2

   Para instancias de Linux, consulte el siguiente ejemplo:

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
    "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   meta-data/iam/security-credentials/role_name
   ```

   Para instancias de Windows, consulte el siguiente ejemplo:

   ```
   PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-
   ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
   ```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token}
 -Method GET -Uri http://169.254.169.254/latest/meta-data/iam/security-
credentials/role_name
```

IMDSv1

Para instancias de Linux, consulte el siguiente ejemplo:

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/iam/security-
credentials/role_name
```

Para instancias de Windows, consulte el siguiente ejemplo:

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/iam/
security-credentials/role_name
```

Command line

Puede utilizar la AWS CLI para asociar un rol a una instancia durante el lanzamiento. Debe especificar el perfil de instancia en el comando.

Para iniciar una instancia con un rol de IAM (AWS CLI)

1. Ejecute el comando run-instances para iniciar una instancia usando el perfil de instancia. En el siguiente ejemplo se muestra cómo iniciar una instancia con el perfil de instancia.

   ```
   aws ec2 run-instances \
       --image-id ami-11aa22bb \
       --iam-instance-profile Name="s3access-profile" \
       --key-name my-key-pair \
       --security-groups my-security-group \
       --subnet-id subnet-1a2b3c4d
   ```

   También puede utilizar el comando New-EC2Instance de Tools for Windows PowerShell.
2. Si utiliza las acciones de la API de Amazon EC2 en su aplicación, recupere las credenciales de seguridad de AWS que están disponibles en la instancia y úselas para firmar las solicitudes. El SDK de AWS se encarga de ello por usted.

```
curl http://169.254.169.254/latest/meta-data/iam/security-credentials/role_name
```

Asociar un rol de IAM a una instancia

Para asociar un rol de IAM a una instancia que no tiene ningún rol, la instancia puede estar en el estado `stopped` o `running`.

Console

Para asociar un rol de IAM con una instancia

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancias).
3. Seleccione la instancia, elija Acciones, Seguridad, Modificar rol de IAM.
4. Seleccione el rol de IAM que desea asociar con la instancia y elija Guardar.

Command line

Para adjuntar un rol de IAM a una instancia (AWS CLI)

1. Si es preciso, describa sus instancias para obtener el ID de la instancia a la que quiere adjuntar el rol.

```
aws ec2 describe-instances
```

2. Ejecute el comando associate-iam-instance-profile para asociar el rol de IAM a la instancia, especificando el perfil de instancia. Puede utilizar el nombre de recurso de Amazon (ARN) del perfil de instancia o bien puede usar su nombre.

```
aws ec2 associate-iam-instance-profile \
    --instance-id i-1234567890abcdef0 \
    --iam-instance-profile Name="TestRole-1"
```

Ejemplo de respuesta

```
{
    "IamInstanceProfileAssociation": {
```

```
        "InstanceId": "i-1234567890abcdef0",
        "State": "associating",
        "AssociationId": "iip-assoc-0dbd8529a48294120",
        "IamInstanceProfile": {
            "Id": "AIPAJLNLDX3AMYZNWYYAY",
            "Arn": "arn:aws:iam::123456789012:instance-profile/TestRole-1"
        }
    }
}
```

También puede usar los siguientes comandos de las Tools for Windows PowerShell:

- Get-EC2Instance
- Register-EC2IamInstanceProfile

Reemplazar un rol de IAM

Para reemplazar el rol de IAM en una instancia que ya tiene un rol de IAM asociado, la instancia debe estar en el estado `running`. Puede hacerlo si desea cambiar el rol de IAM de una instancia sin disociar primero el existente. Por ejemplo, puede hacer esto para asegurarse de que no se interrumpan las acciones de API realizadas por las aplicaciones que se ejecutan en la instancia.

Console

Para reemplazar un rol de IAM de una instancia

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancias).
3. Seleccione la instancia, elija Acciones, Seguridad, Modificar rol de IAM.
4. Seleccione el rol de IAM que desea asociar con la instancia y elija Guardar.

Command line

Para reemplazar un rol de IAM de una instancia (AWS CLI)

1. Si es necesario, describa sus asociaciones de perfil de instancia de IAM para obtener el ID de asociación del perfil de instancia de IAM que quiere reemplazar.

```
aws ec2 describe-iam-instance-profile-associations
```

2. Utilice el comando replace-iam-instance-profile-association para sustituir el perfil de instancia de IAM especificando el ID de asociación del perfil de instancia ya existente y el ARN o el nombre del perfil de instancia que debe sustituirlo.

```
aws ec2 replace-iam-instance-profile-association \
    --association-id iip-assoc-0044d817db6c0a4ba \
    --iam-instance-profile Name="TestRole-2"
```

Ejemplo de respuesta

```
{
    "IamInstanceProfileAssociation": {
        "InstanceId": "i-087711ddaf98f9489",
        "State": "associating",
        "AssociationId": "iip-assoc-09654be48e33b91e0",
        "IamInstanceProfile": {
            "Id": "AIPAJCJEDKX7QYHWYK7GS",
            "Arn": "arn:aws:iam::123456789012:instance-profile/TestRole-2"
        }
    }
}
```

También puede usar los siguientes comandos de las Tools for Windows PowerShell:

- Get-EC2IamInstanceProfileAssociation
- Set-EC2IamInstanceProfileAssociation

Separar un rol de IAM

Puede separar un rol de IAM de una instancia en ejecución o detenida.

Console

Para separar un rol de IAM de una instancia

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

2. En el panel de navegación, seleccione Instances (Instancias).
3. Seleccione la instancia, elija Actions (Acciones), Security (Seguridad), Modify IAM role (Modificar rol de IAM).
4. En Rol de IAM, elija Sin rol de IAM. Seleccione Save.
5. En el cuadro de diálogo de confirmación, escriba Desasociar y, a continuación, elija Desasociar.

Command line

Para desconectar un rol de IAM de una instancia (AWS CLI)

1. Si es necesario, utilice describe-iam-instance-profile-associations para describir sus asociaciones de perfil de instancia de IAM y obtener el ID de asociación del perfil de instancia de IAM que va a desasociar.

```
aws ec2 describe-iam-instance-profile-associations
```

Ejemplo de respuesta

```
{
    "IamInstanceProfileAssociations": [
        {
            "InstanceId": "i-088ce778fbfeb4361",
            "State": "associated",
            "AssociationId": "iip-assoc-0044d817db6c0a4ba",
            "IamInstanceProfile": {
                "Id": "AIPAJEDNCAA64SSD265D6",
                "Arn": "arn:aws:iam::123456789012:instance-profile/TestRole-2"
            }
        }
    ]
}
```

2. Utilice el comando disassociate-iam-instance-profile para desasociar el perfil de instancia de IAM utilizando su ID de asociación.

```
aws ec2 disassociate-iam-instance-profile --association-id iip-
assoc-0044d817db6c0a4ba
```

Ejemplo de respuesta

```
{
    "IamInstanceProfileAssociation": {
        "InstanceId": "i-087711ddaf98f9489",
        "State": "disassociating",
        "AssociationId": "iip-assoc-0044d817db6c0a4ba",
        "IamInstanceProfile": {
            "Id": "AIPAJEDNCAA64SSD265D6",
            "Arn": "arn:aws:iam::123456789012:instance-profile/TestRole-2"
        }
    }
}
```

También puede usar los siguientes comandos de las Tools for Windows PowerShell:

- Get-EC2IamInstanceProfileAssociation
- Unregister-EC2IamInstanceProfile

Generar una política para su rol de IAM basada en la actividad de acceso

Cuando crea por primera vez un rol de IAM para las aplicaciones, a veces puede conceder permisos más allá de lo necesario. Antes de iniciar la aplicación en su entorno de producción, puede generar una política de IAM que esté basada en la actividad de acceso de un rol de IAM. El analizador de acceso de IAM revisa los registros de AWS CloudTrail y genera una plantilla de política que contiene los permisos que ha utilizado el rol en el intervalo de fechas especificado. Puede utilizar la plantilla para crear una política administrada con permisos detallados y, a continuación, adjuntarla al rol de IAM. De esta forma, solo concede los permisos que el rol necesita para interactuar con los recursos de AWS para su caso de uso específico. Esto le ayuda a cumplir con la mejor práctica de otorgar privilegios mínimos. Para obtener más información, consulte Generar políticas basadas en la actividad de acceso en la Guía del usuario de IAM.

Acceso a Amazon EC2 mediante un punto de conexión de VPC de interfaz.

Para mejorar la posición de seguridad de su VPC, cree una conexión privada entre su VPC y Amazon EC2. Puede acceder a Amazon EC2 como si estuviera en su VPC, sin el uso de una puerta

de enlace de Internet, un dispositivo NAT, una conexión VPN o una conexión AWS Direct Connect. Las instancias de la VPC no necesitan direcciones IP públicas para acceder a Amazon EC2.

Para obtener más información, consulte Acceso a Servicios de AWS a través de AWS PrivateLink en la Guía de AWS PrivateLink.

Contenido

Creación de un punto de conexión de la VPC de tipo interfaz

Cree un punto de conexión para Amazon EC2 con el siguiente nombre de servicio:

- com.amazonaws.***región***.ec2: crea un punto de conexión para las acciones de la API de Amazon EC2.

Para obtener más información, consulte Acceder a Servicio de AWS a través de un punto de conexión de VPC de interfaz en la Guía de AWS PrivateLink.

Creación de una política de punto de conexión

Una política de punto de conexión es un recurso de IAM que puede adjuntar al punto de conexión de su interfaz. La política de punto de conexión predeterminada permite acceso completo a la API de Amazon EC2 a través del punto de conexión de interfaz. Para controlar el acceso permitido a la API de Amazon EC2 desde la VPC, adjunte una política de punto de conexión personalizada al punto de conexión de interfaz.

Una política de punto de conexión especifica la siguiente información:

- Las entidades principales que pueden realizar acciones.
- Las acciones que se pueden realizar.
- El recurso en el que se pueden realizar las acciones.

> **Important**
>
> Cuando se aplica una política no predeterminada a un punto de conexión de VPC de interfaz de Amazon EC2, es posible que algunas solicitudes de API que produzcan un error, como aquellas que fallan a partir de `RequestLimitExceeded`, no estén registradas en AWS CloudTrail o Amazon CloudWatch.

Para obtener más información, consulte Control del acceso a los servicios con puntos de conexión de la VPC en la Guía del usuario de AWS PrivateLink.

En el ejemplo siguiente se muestra una política de punto de conexión de VPC que deniega el permiso para crear volúmenes no cifrados o para lanzar instancias con volúmenes no cifrados. La política de ejemplo también concede permiso para realizar todas las demás acciones de Amazon EC2.

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
        "Action": "ec2:*",
        "Effect": "Allow",
        "Resource": "*",
        "Principal": "*"
    },
    {
        "Action": [
            "ec2:CreateVolume"
        ],
        "Effect": "Deny",
        "Resource": "*",
        "Principal": "*",
        "Condition": {
            "Bool": {
                "ec2:Encrypted": "false"
            }
        }
    },
    {
        "Action": [
            "ec2:RunInstances"
```

```
        ],
        "Effect": "Deny",
        "Resource": "*",
        "Principal": "*",
        "Condition": {
            "Bool": {
                "ec2:Encrypted": "false"
            }
        }
    }]
}
```

Administración de actualizaciones para instancias de Windows de Amazon EC2

Le recomendamos que aplique parches al sistema operativo y a las aplicaciones, los actualice periódicamente y los proteja en sus instancias de EC2. Puede usar AWS Systems Manager Patch Manager para automatizar el proceso de instalar actualizaciones relacionadas con la seguridad tanto para el sistema operativo como para las aplicaciones.

En el caso de las instancias de EC2 de un grupo de escalamiento automático, puede utilizar el runbook AWS-PatchAsgInstance para evitar que se sustituyan instancias en las que se están aplicando parches. De forma alternativa, puede usar cualquier servicio de actualización automática u otros procesos recomendados para instalar actualizaciones que proporciona el proveedor de la aplicación.

Recursos

- AL2023: Actualización de AL2023 en la Guía del usuario de Amazon Linux 2023.
- AL2: Administración del software de su instancia de Amazon Linux 2 en la Guía del usuario de Amazon Linux 2.
- Instancias de Windows: the section called “Administración de actualizaciones”.

Prácticas recomendadas de seguridad para instancias de Windows

Recomendamos que siga estas prácticas recomendadas de seguridad para las instancias de Windows.

Contenido

Prácticas recomendadas de seguridad de alto nivel

Debe cumplir las siguientes prácticas recomendadas de seguridad de alto nivel en sus instancias de Windows:

- Acceso mínimo: otorgue acceso solo a los sistemas y ubicaciones de confianza y esperados. Esto se aplica a todos los productos de Microsoft, por ejemplo, Active Directory, servidores de productividad empresarial de Microsoft y servicios de infraestructura como servicios de Escritorio remoto, servidores proxy inverso, servidores web IIS, entre otros. Utilice las capacidades de AWS tales como los grupos de seguridad de instancias de Amazon EC2, las listas de control de acceso (ACL) a la red y las subredes públicas/privadas de Amazon VPC para separar la seguridad en capas en varias ubicaciones de una arquitectura. Dentro de una instancia de Windows, los clientes pueden usar el Firewall de Windows para aplicar una estrategia de defensa en profundidad dentro de su implementación. Instale solo los componentes del sistema operativo y las aplicaciones que sean necesarios para que el sistema funcione según el diseño. Configure servicios de infraestructura como IIS para que se ejecuten en cuentas de servicio o para que utilicen características como identidades del grupo de aplicaciones que permitan acceder a los recursos de forma local y remota en toda la infraestructura.
- Privilegio mínimo: determine el conjunto mínimo de privilegios que las instancias y las cuentas necesitan para realizar sus funciones. Limite estos servidores y usuarios para que permitan únicamente dichos permisos definidos. Utilice técnicas como Controles de acceso basados en roles para reducir el área superficial de las cuentas administrativas y crear los roles más limitados para realizar una tarea. Utilice características del sistema operativo como el sistema de archivos cifrados (EFS) dentro de NTFS para cifrar información confidencial en reposo y controlar el acceso de aplicaciones y usuarios a ella.
- Administración de configuración: cree una configuración de servidor de línea de base que incorpore parches de seguridad actualizados y conjuntos de protección basados en host que incluyan antivirus, antimalware, detección/prevención de intrusiones y monitoreo de la integridad

de archivos. Evalúe cada servidor con respecto a la referencia registrada actual para identificar y marcar cualquier desviación. Asegúrese de que cada servidor esté configurado para generar y almacenar de forma segura los datos adecuados de registro y auditoría.

- Administración de cambios: cree procesos para controlar los cambios en las referencias de configuración del servidor y trabaje en procesos de cambio totalmente automatizados. Además, aproveche Just Enough Administration (JEA) con Windows PowerShell DSC para limitar el acceso administrativo a las funciones mínimas requeridas.
- Gestión de parches: implemente procesos que corrigen, actualizan y protegen con regularidad el sistema operativo y las aplicaciones de sus instancias EC2.
- Registros de auditoría: audite el acceso y todos los cambios en las instancias de Amazon EC2 para verificar la integridad del servidor y asegurarse de que solo se realicen los cambios autorizados. Aproveche características como el Registro mejorado para IIS para mejorar las capacidades de registro predeterminadas. Capacidades de AWS como los registros de flujo de VPC y también AWS CloudTrail están disponibles para auditar el acceso a la red, incluidas las solicitudes permitidas/denegadas y las llamadas a la API, respectivamente.

Administración de actualizaciones

Se recomienda llevar a cabo las siguientes prácticas recomendadas si desea obtener los mejores resultados al ejecutar Windows Server en Amazon EC2:

- Configure Windows Update
- Update drivers
- Use the latest Windows AMIs
- Test performance before migration
- Update launch agents
- Reinicie una instancia de Windows después de instalar las actualizaciones. Para obtener más información, consulte Reinicio de su instancia.

Para obtener información acerca de cómo actualizar o migrar una instancia de Windows a una versión más reciente de Windows Server, consulte Actualizar una instancia de Windows Amazon EC2 a una versión más reciente de Windows Server.

Configuración de Windows Update

De forma predeterminada, las instancias que se inician desde las AMI de Windows Server de AWS no reciben actualizaciones a través de Windows Update.

Actualización de los controladores de Windows

Mantenga actualizados los controladores en todas las instancias de EC2 de Windows para asegurarse de aplicar las correcciones de problemas y mejoras de rendimiento más recientes en toda la flota. Según el tipo de instancia, debe actualizar los controladores de AWS PV, Amazon ENA y AWS NVMe.

- Utilice los temas de SNS para recibir las actualizaciones de las nuevas versiones de los controladores.
- Use el manual de procedimientos de Automation AWS Systems Manager AWSSupport-UpgradeWindowsAWSDrivers para poder aplicar las actualizaciones fácilmente en sus instancias.

Lanzamiento de instancias con las últimas AMI de Windows

AWS publica nuevas AMI de Windows todos los meses, que contienen los últimos parches del sistema operativo, controladores y agentes de lanzamiento. Aproveche las AMI más recientes al lanzar nuevas instancias o al crear sus propias imágenes personalizadas.

- Para consultar las actualizaciones de cada versión de las AMI de Windows de AWS, consulte el Historial de versiones de las AMI de Windows de AWS.
- Para utilizar las AMI más recientes disponibles, consulte el artículo sobre cómo encontrar las AMI de Windows más recientes con el almacén de parámetros de Systems Manager.
- Para obtener más información sobre las AMI de Windows especializadas que puede usar a fin de lanzar instancias para su base de datos y los casos de uso de refuerzo de la conformidad, consulte AMI de Windows especializadas en la Referencia de AMI de Windows de AWS.

Prueba del rendimiento del sistema o de la aplicación antes de la migración

La migración de aplicaciones empresariales a AWS puede implicar numerosas variables y configuraciones. Realice siempre una prueba de rendimiento de la solución de EC2 para asegurarse de que:

- Los tipos de instancias están bien configurados, incluido el tamaño de la instancia, las redes mejoradas y la tenencia (compartida o dedicada).

- La topología de la instancia es adecuada para la carga de trabajo y aprovecha las características de alto rendimiento cuando es necesario, como la tenencia dedicada, los grupos de ubicación, los volúmenes del almacén de instancias, los bare metal.

Actualización de los agentes de lanzamiento

Actualice al agente de EC2Launch v2 más reciente para asegurarse de que las últimas mejoras se apliquen en toda la flota. Para obtener más información, consulte the section called “Migración”.

Si tiene una flota mixta o si desea seguir usando los agentes de EC2Launch (Windows Server 2016 y 2019) o de EC2 Config (solo sistema operativo heredado), actualice a las versiones más recientes de los respectivos agentes.

Las siguientes combinaciones de agentes de lanzamiento y versión de Windows Server admiten actualizaciones automáticas. Puede optar por las actualizaciones automáticas en la consola de administración de host con Quick Setup de SSM, en Agentes de lanzamiento de Amazon EC2.

Versión de Windows	EC2Launch v1	EC2Launch v2
2016	✓	✓
2019	✓	✓
2022		✓

- Para obtener más información acerca de la actualización a EC2Launch v2, consulte the section called “Instalar”.
- Para obtener información sobre cómo actualizar manualmente EC2Config, consulte. the section called “Instalar EC2config”
- Para obtener información sobre cómo actualizar manualmente EC2Launch, consulte. the section called “Instalar EC2Launch”

Administración de la configuración

Las Imágenes de máquina de Amazon (AMI) proporcionan una configuración inicial para una instancia Amazon EC2, que incluye el sistema operativo Windows y personalizaciones opcionales

específicas del cliente, como aplicaciones y controles de seguridad. Cree un catálogo de AMI que contenga líneas de base de configuración de seguridad personalizadas para garantizar que todas las instancias de Windows se inicien con controles de seguridad estándar. Las líneas de base de seguridad se pueden convertir en una AMI, arrancar de forma dinámica cuando se lanza una instancia de EC2 o empaquetar como producto para una distribución uniforme a través de las carteras de AWS Service Catalog. Para obtener más información sobre cómo proteger una AMI, consulte las prácticas recomendadas para crear una AMI.

Cada instancia Amazon EC2 debe cumplir con los estándares de seguridad de la organización. No instale roles y características de Windows que no sean necesarias, e instale software para protegerse contra código malintencionado (antivirus, antimalware, mitigación de vulnerabilidades), monitorear la integridad del host y detectar intrusiones. Configure el software de seguridad para monitorear y mantener la configuración de seguridad del sistema operativo, proteger la integridad de los archivos críticos del sistema operativo y alertar sobre las desviaciones de la línea de base de seguridad. Considere la posibilidad de implementar los parámetros de configuración de seguridad recomendados publicados por Microsoft, el Center for Internet Security (CIS) o el Instituto Nacional de Normalización y Tecnología (NIST). Considere la posibilidad de utilizar otras herramientas de Microsoft para determinados servidores de aplicaciones, como el Analizador de prácticas recomendadas para SQL Server.

Los clientes de AWS también pueden ejecutar evaluaciones de Amazon Inspector para mejorar la seguridad y la conformidad de las aplicaciones implementadas en instancias de Amazon EC2. Amazon Inspector evalúa automáticamente las aplicaciones en busca de vulnerabilidades o desviaciones de las prácticas recomendadas e incluye una base de conocimientos de cientos de reglas mapeadas a estándares comunes de conformidad de seguridad (por ejemplo, PCI DSS) y definiciones de vulnerabilidades. Entre los ejemplos de reglas integradas se incluye comprobar si el inicio de sesión raíz remoto está habilitado o si hay versiones de software vulnerables instaladas. Los investigadores de seguridad de AWS actualizan estas reglas con regularidad.

Al proteger instancias de Windows, se recomienda implementar los servicios de dominio de Active Directory para habilitar una infraestructura escalable, segura y administrable para ubicaciones distribuidas. Además, después de lanzar instancias a través de la consola de Amazon EC2 o mediante una herramienta de aprovisionamiento de Amazon EC2, como AWS CloudFormation, es recomendable utilizar características nativas del sistema operativo, como Microsoft Windows PowerShell DSC para mantener el estado de configuración en caso de que se produzca una desviación de esta.

Administración de cambios

Después de aplicar las líneas base de seguridad iniciales a las instancias Amazon EC2 en el lanzamiento, controle los cambios en curso en Amazon EC2 para mantener la seguridad de las máquinas virtuales. Establezca un proceso de administración de cambios para autorizar e incorporar cambios en los recursos de AWS (como grupos de seguridad, tablas de enrutamiento y ACL de red), así como en las configuraciones del SO y las aplicaciones (como la aplicación de parches de Windows o aplicaciones, actualizaciones de software o actualizaciones de archivos de configuración).

AWS proporciona varias herramientas para ayudar a administrar los cambios en los recursos de AWS, incluidos AWS CloudTrail, AWS Config, AWS CloudFormation y AWS Elastic Beanstalk. AWS OpsWorks y paquetes de administración para Systems Center Operations Manager y System Center Virtual Machine Manager. Tenga en cuenta que Microsoft publica revisiones de Windows todos los martes (a veces incluso diariamente) y AWS actualiza todas las AMI de Windows administradas por AWS dentro de los cinco días siguientes a que Microsoft publique un parche. Por lo tanto, es importante aplicar parches continuamente a todas las AMI de línea de base, actualizar las plantillas de AWS CloudFormation y las configuraciones de grupo de Auto Scaling con los últimos ID de AMI e implementar herramientas para automatizar la administración de parches de instancia en ejecución.

Microsoft proporciona varias opciones para administrar el sistema operativo Windows y los cambios en las aplicaciones. SCCM, por ejemplo, proporciona una cobertura completa del ciclo de vida de las modificaciones del entorno. Seleccione herramientas que aborden los requisitos empresariales y controlen cómo los cambios afectarán los SLA de las aplicaciones, la capacidad, la seguridad y los procedimientos de recuperación de desastres. Evite los cambios manuales y, en su lugar, aproveche el software de administración de configuración automatizada o las herramientas de línea de comandos, como EC2 Run Command o Windows PowerShell para implementar procesos de cambio repetibles y con secuencias de comandos. Para facilitar este requisito, utilice hosts de bastión con registro mejorado para todas las interacciones con las instancias de Windows para asegurarse de que todos los eventos y tareas se graben automáticamente.

Auditoría y rendición de cuentas para instancias de Windows de Amazon EC2

AWS CloudTrail, AWS Config y Reglas de AWS Config proporcionar características de auditoría y seguimiento de cambios para auditar los cambios de recursos de AWS. Configure los registros de eventos de Windows para enviar archivos de registro locales a un sistema de administración

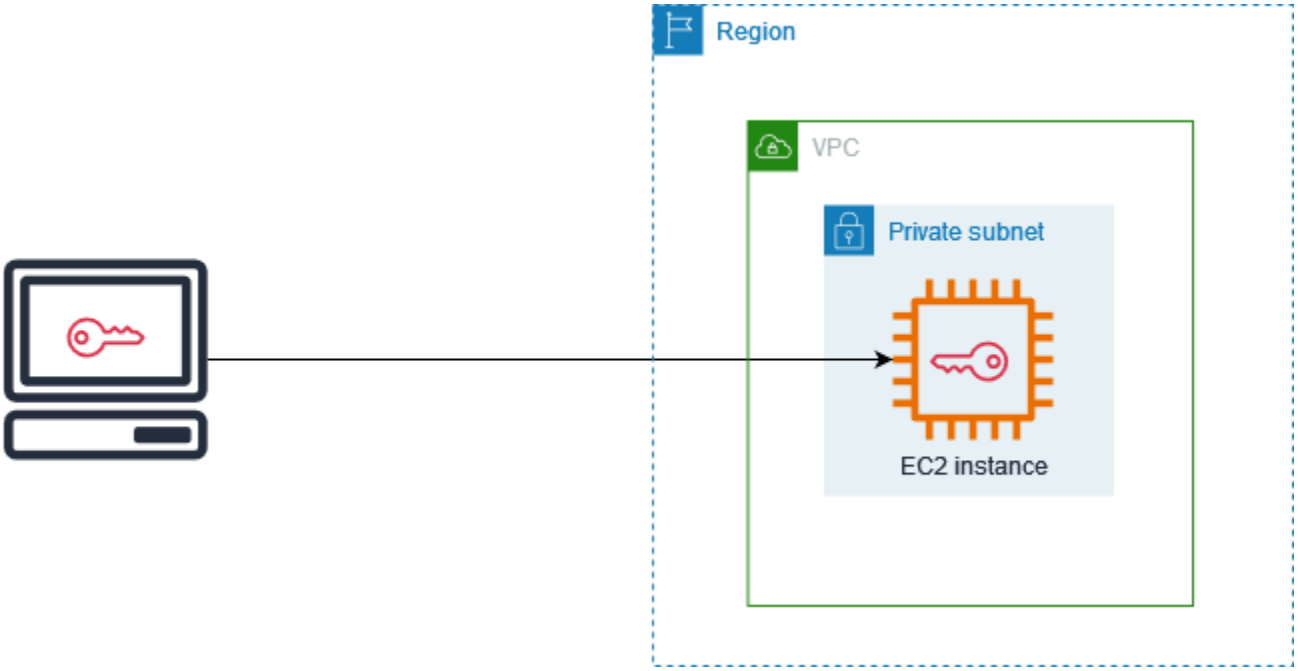
de registros centralizado para conservar los datos de registro para el análisis de seguridad y comportamiento operativo. Microsoft System Center Operations Manager (SCOM) agrega información acerca de las aplicaciones de Microsoft implementadas en instancias de Windows y aplica conjuntos de reglas preconfigurados y personalizados basados en roles y servicios de aplicaciones. Los System Center Management Packs se basan en SCOM para proporcionar monitoreo y orientación de configuración específicos de las aplicaciones. Estos paquetes de administración admiten Windows Server Active Directory, SharePoint Server 2013, Exchange Server 2013, Lync Server 2013, SQL Server 2014 y muchos otros servidores y tecnologías.

Además de las herramientas de administración de sistemas de Microsoft, los clientes pueden utilizar Amazon CloudWatch para monitorear la utilización de la CPU de instancias, el rendimiento del disco, la E/S de red y realizar comprobaciones de estado de hosts e instancias. Los agentes de lanzamiento EC2Config, EC2Launch y EC2Launch v2 proporcionan acceso a características avanzadas adicionales para las instancias de Windows. Por ejemplo, pueden exportar registros de sistemas, seguridad, aplicaciones e Internet Information Services (IIS) de Windows a CloudWatch Logs que se pueden integrar con métricas y alarmas de Amazon CloudWatch. Los clientes también pueden crear scripts que exporten contadores de rendimiento de Windows a métricas personalizadas de Amazon CloudWatch.

Pares de claves e instancias de Amazon EC2

Un par de claves, que consta de una clave pública y una clave privada, es un conjunto de credenciales de seguridad que se utiliza para demostrar su identidad cuando se conecta a una instancia de Amazon EC2. En el caso de las instancias de Linux, la clave privada le permite utilizar SSH para conectarse de forma segura a la instancia. Para las instancias de Windows, se requiere la clave privada para descifrar la contraseña del administrador, que después utilizará para conectarse a la instancia.

Amazon EC2 almacena la clave pública en su instancia y usted almacena la clave privada, como se muestra en el diagrama siguiente. Es importante que almacene su clave privada en un lugar seguro, ya que cualquier persona que la tenga puede conectarse a las instancias que utilizan el par de claves.



Cuando lanza una instancia, puede especificar un par de claves para poder conectarse a la instancia mediante un método que requiera un par de claves. Según cómo administre la seguridad, puede especificar el mismo par de claves para todas las instancias o puede especificar pares de claves diferentes.

Para instancias de Linux, cuando la instancia se arranca por primera vez, la clave pública que especificó durante el lanzamiento se coloca en la instancia de Linux en una entrada dentro de `~/.ssh/authorized_keys`. Cuando se conecta a su instancia de Linux mediante SSH, debe especificar la clave privada que corresponde a la clave pública para iniciar sesión.

Para obtener más información sobre cómo conectarse a la instancia EC2, consulte Conexión con instancias EC2.

> **Important**
>
> Debido a que Amazon EC2 no conserva una copia de su clave privada, no hay ningún modo de recuperar una clave privada si se pierde. Sin embargo, todavía puede haber una forma de conectarse a instancias para las que ha perdido la clave privada. Para obtener más información, consulte Perdí mi clave privada. ¿Cómo puedo conectarme a mi instancia de Linux?.

Como alternativa a los pares de claves, puede utilizar AWS Systems Manager Session Manager para conectarse a su instancia con un shell interactivo de un solo clic basado en navegador o la AWS Command Line Interface (AWS CLI).

Contenido

Creación de un par de claves para la instancia de Amazon EC2

Puede utilizar Amazon EC2 para crear los pares de claves, o bien usar una herramienta de terceros para crearlos e importarlos luego en Amazon EC2.

Amazon EC2 admite claves RSA SSH-2 de 2048 bits para instancias de Linux y Windows. Amazon EC2 también admite claves ED25519 para las instancias de Linux.

Para conocer cómo puede conectarse a una instancia de Linux mediante SSH después de crear un par de claves, consulte the section called “Conexión con la instancia de Linux”.

Para conocer cómo puede conectarse a una instancia de Windows mediante RDP después de crear un par de claves, consulte the section called “Conexión con la instancia de Windows de”.

Contenido

Crear un par de claves mediante Amazon EC2

Cuando se crea un par de claves con Amazon EC2, la clave pública se almacena en Amazon EC2, y usted almacena la clave privada.

Puede crear hasta 5000 pares de claves por región. Para solicitar un aumento, cree un caso de asistencia. Para obtener más información, consulte Creación de un caso de soporte en la Guía del usuario de AWS Support.

Console

Para crear un par de claves mediante Amazon EC2

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Network & Security, seleccione Key Pairs.
3. Elija Create key pair (Crear par de claves).
4. En Nombre, escriba un nombre descriptivo para el par de claves. Amazon EC2 asocia la clave pública al nombre que especifique como nombre de la clave. El nombre de una clave puede incluir hasta 255 caracteres ASCII. No puede incluir espacios iniciales ni finales.
5. Seleccione un tipo de par de claves adecuado para su sistema operativo:

   (Instancias de Linux) En Tipo de par de claves, elija RSA o ED25519.

   (Instancias de Windows) En Tipo de par de claves, elija RSA. Las claves ED25519 no son compatibles con instancias de Windows.
6. En Formato de archivo de la clave privada, elija el formato en el que desea guardar la clave privada. Para guardar la clave privada en un formato que se pueda utilizar con OpenSSH, elija pem. Para guardar la clave privada en un formato que se pueda utilizar con PuTTY, elija ppk.
7. Para agregar una etiqueta a la clave pública, elija Agregar etiqueta e ingrese la clave y el valor de la etiqueta. Repita este proceso para cada etiqueta.
8. Elija Crear par de claves.
9. Su navegador descargará el archivo de clave privada automáticamente. El nombre del archivo base es el nombre especificado como el nombre del par de claves y la extensión del nombre de archivo la determina el formato de archivo elegido. Guarde el archivo de clave privada en un lugar seguro.

   > **Important**
   >
   > Esta es la única oportunidad para guardar el archivo de clave privada.

10. (Instancias de Linux) Si tiene planeado usar un cliente SSH en un equipo macOS o Linux para conectarse a su instancia de Linux, utilice el comando a continuación para establecer los permisos de su archivo de clave privada de manera que solo usted pueda leerlo.

```
chmod 400 key-pair-name.pem
```

Si no configura estos permisos, no podrá conectarse a la instancia con este par de claves. Para obtener más información, consulte Error: Unprotected Private Key File (Error: archivo de clave privada no protegido).

AWS CLI

Para crear un par de claves mediante Amazon EC2

1. Utilice el comando create-key-pair como se indica a continuación para generar el par de claves y guardar la clave privada en un archivo `.pem`.

   En `--key-name`, especifique un nombre para la clave pública. El nombre puede incluir hasta 255 caracteres ASCII.

   En `--key-type`, especifique `rsa` o `ed25519`. Si no incluye el parámetro `--key-type`, se crea una clave `rsa` de forma predeterminada. Tenga en cuenta que las claves ED25519 no son compatibles con instancias de Windows.

   En `--key-format`, especifique `pem` o `ppk`. Si no incluye el parámetro `--key-format`, se crea un archivo `pem` de forma predeterminada.

   `--query "KeyMaterial"` imprime el material de clave privada en la salida.

   `--output text > my-key-pair.pem` guarda el material de clave privada en un archivo con la extensión especificada. La extensión puede ser `.pem` o `.ppk`. La clave privada puede tener un nombre diferente del nombre de la clave pública, pero para facilitar su uso, utilice el mismo nombre.

```
aws ec2 create-key-pair \
    --key-name my-key-pair \
    --key-type rsa \
    --key-format pem \
    --query "KeyMaterial" \
```

```
    --output text > my-key-pair.pem
```

2. (Instancias de Linux) Si tiene planeado usar un cliente SSH en un equipo macOS o Linux para conectarse a su instancia de Linux, utilice el comando a continuación para establecer los permisos de su archivo de clave privada de manera que solo usted pueda leerlo.

   ```
   chmod 400 key-pair-name.pem
   ```

   Si no configura estos permisos, no podrá conectarse a la instancia con este par de claves. Para obtener más información, consulte Error: Unprotected Private Key File (Error: archivo de clave privada no protegido).

PowerShell

Para crear un par de claves mediante Amazon EC2

Utilice el comando New-EC2KeyPair de AWS Tools for Windows PowerShell como se indica a continuación para generar la clave y guardarla en un archivo `.pem` o `.ppk`.

En `-KeyName`, especifique un nombre para la clave pública. El nombre puede incluir hasta 255 caracteres ASCII.

En `-KeyType`, especifique `rsa` o `ed25519`. Si no incluye el parámetro `-KeyType`, se crea una clave `rsa` de forma predeterminada. Tenga en cuenta que las claves ED25519 no son compatibles con instancias de Windows.

En `-KeyFormat`, especifique `pem` o `ppk`. Si no incluye el parámetro `-KeyFormat`, se crea un archivo `pem` de forma predeterminada.

`KeyMaterial` imprime el material de clave privada en la salida.

`Out-File -Encoding ascii -FilePath C:\path\my-key-pair.pem` guarda el material de clave privada en un archivo con la extensión especificada. La extensión puede ser `.pem` o `.ppk`. La clave privada puede tener un nombre diferente del nombre de la clave pública, pero para facilitar su uso, utilice el mismo nombre.

```
PS C:\> (New-EC2KeyPair -KeyName "my-key-pair" -KeyType "rsa" -KeyFormat
 "pem").KeyMaterial | Out-File -Encoding ascii -FilePath C:\path\my-key-pair.pem
```

Crear un par de claves con AWS CloudFormation

Cuando crea un nuevo par de claves con AWS CloudFormation, la clave privada se guarda en un almacén de parámetros de AWS Systems Manager. El formato del nombre del parámetro es el siguiente:

```
/ec2/keypair/key_pair_id
```

Para obtener más información, consulte Almacén de parámetros de AWS Systems Manager en la Guía del usuario de AWS Systems Manager.

Para crear un par de claves con AWS CloudFormation

1. Especifique el recurso AWS::EC2::KeyPair en su plantilla.

   ```
   Resources:
     NewKeyPair:
       Type: 'AWS::EC2::KeyPair'
       Properties:
         KeyName: new-key-pair
   ```

2. Utilice el comando describe-key-pairs como se indica a continuación para obtener el ID del par de claves.

   ```
   aws ec2 describe-key-pairs --filters Name=key-name,Values=new-key-pair --query
    KeyPairs[*].KeyPairId --output text
   ```

   A continuación, se muestra un ejemplo del resultado.

   ```
   key-05abb699beEXAMPLE
   ```

3. Utilice el comando get-parameter como se indica a continuación para obtener el parámetro de su clave y guardar el material de la clave en un archivo `.pem`.

   ```
   aws ssm get-parameter --name /ec2/keypair/key-05abb699beEXAMPLE --with-decryption
    --query Parameter.Value --output text > new-key-pair.pem
   ```

Permisos de IAM necesarios

Para que AWS CloudFormation pueda administrar los parámetros del Almacén de parámetros en su nombre, el rol de IAM asumido por AWS CloudFormation o su usuario tiene que tener los permisos siguientes:

- `ssm:PutParameter`: otorga permiso para crear un parámetro para el material de clave privada.
- `ssm:DeleteParameter`: concede permiso para eliminar el parámetro que almacenaba el material de la clave privada. Este permiso es necesario independientemente de si AWS CloudFormation creó o importó el par de claves.

Cuando AWS CloudFormation elimina un par de claves que la pila creó o importó, hace una comprobación de los permisos para determinar si tiene permiso para eliminar parámetros, aunque AWS CloudFormation crea un parámetro solo cuando crea un par de claves, no cuando importa un par de claves. AWS CloudFormation comprueba el permiso necesario mediante un nombre de parámetro inventado que no coincide con ningún parámetro de su cuenta. Por lo tanto, es posible que vea un nombre de parámetro inventado en el mensaje de error `AccessDeniedException`.

Crear un par de claves con una herramienta de terceros e importar la clave pública a Amazon EC2

instancias de Linux

En lugar de utilizar Amazon EC2 para crear un par de claves, puede crear un par de claves RSA o ED25519 con una herramienta de terceros y, a continuación, importar la clave pública en Amazon EC2.

Requisitos para pares de claves

- Tipos compatibles: RSA y ED25519. Amazon EC2 no acepta claves DSA.
- Formatos admitidos:
  - Formato de clave pública de OpenSSH (formato de `~/.ssh/authorized_keys`). Si se conecta mediante SSH mientras utiliza la API de EC2 Instance Connect, se admite también el formato SSH.
  - El formato del archivo de clave privada de SSH debe ser PEM o PPK
  - (Solo RSA) Formato DER codificado en Base64
  - (Solo RSA) Formato de archivo de claves públicas de SSH tal y como se especifica en RFC 4716

- Las longitudes admitidas son 1024, 2048 y 4096. Si se conecta mediante SSH mientras utiliza la API de EC2 Instance Connect, se admiten las longitudes 2048 y 4096.

Para crear su par de claves con una herramienta de terceros

1. Genere un par de claves con la herramienta de terceros de su elección. Por ejemplo, puede usar ssh-keygen (una herramienta proporcionada con la instalación de OpenSSH estándar). Además, Java, Ruby, Python y otros muchos lenguajes de programación ofrecen bibliotecas estándar que puede utilizar para crear un par de claves RSA o ED25519.

   > **Important**
   >
   > La clave privada debe estar en formato PEM o PPK. Por ejemplo, use `ssh-keygen -m PEM` para generar la clave OpenSSH en el formato PEM.

2. Guarde la clave pública en un archivo local. Por ejemplo, `~/.ssh/my-key-pair.pub`. La extensión de este archivo no es importante.
3. Guarde la clave privada en un archivo local con la extensión `.pem` o `.ppk`. Por ejemplo, `~/.ssh/my-key-pair.pem` o `~/.ssh/my-key-pair.ppk`.

   > **Important**
   >
   > Guarde el archivo de clave privada en un lugar seguro. Deberá proporcionar el nombre de su clave pública al iniciar una instancia y la clave privada correspondiente cada vez que se conecte a dicha instancia.

instancias de Windows

En lugar de utilizar Amazon EC2 para crear el par de claves, puede crear un par de claves RSA con una herramienta de terceros, y luego importar la clave pública en Amazon EC2.

Requisitos para pares de claves

- Tipos compatibles: RSA Amazon EC2 no acepta claves DSA.

> **Note**
>
> Las claves ED25519 no son compatibles con instancias de Windows.

- Formatos admitidos:
  - Formato de clave pública de OpenSSH
  - El formato del archivo de clave privada de SSH debe ser PEM o PPK
  - (Solo RSA) Formato DER codificado en Base64
  - (Solo RSA) Formato de archivo de claves públicas de SSH tal y como se especifica en RFC 4716
- Las longitudes admitidas son 1024, 2048 y 4096.

Para crear su par de claves con una herramienta de terceros

1. Genere un par de claves con la herramienta de terceros de su elección. Por ejemplo, puede usar ssh-keygen (una herramienta proporcionada con la instalación de OpenSSH estándar). Además, Java, Ruby, Python y otros muchos lenguajes de programación ofrecen bibliotecas estándar que puede utilizar para crear un par de claves RSA.

   > **Important**
   >
   > La clave privada debe estar en formato PEM o PPK. Por ejemplo, use `ssh-keygen -m PEM` para generar la clave OpenSSH en el formato PEM.

2. Guarde la clave pública en un archivo local. Por ejemplo, `C:\keys\my-key-pair.pub`. La extensión de este archivo no es importante.
3. Guarde la clave privada en un archivo local con la extensión `.pem` o `.ppk`. Por ejemplo, `C:\keys\my-key-pair.pem` o `C:\keys\my-key-pair.ppk`. La extensión del nombre de archivo es importante porque solo se pueden seleccionar archivos `.pem` al conectarse a la instancia de Windows desde la consola de EC2.

> **Important**
>
> Guarde el archivo de clave privada en un lugar seguro. Deberá proporcionar el nombre de su clave pública al iniciar una instancia y la clave privada correspondiente cada vez que se conecte a dicha instancia.

Una vez creado el par de claves, use uno de los métodos siguientes para importar la clave pública a Amazon EC2.

Console

Para importar la clave pública a Amazon EC2

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Key Pairs (Pares de claves).
3. Elija Importar par de claves.
4. En Nombre, escriba un nombre descriptivo para la clave pública. El nombre puede incluir hasta 255 caracteres ASCII. No puede incluir espacios iniciales ni finales.

   > **Note**
   >
   > Cuando se conecta a la instancia desde la consola de EC2, dicha consola sugiere este nombre para el nombre del archivo de clave privada.

5. Elija Examinar para desplazarse hasta la clave pública y seleccionarla, o pegue el contenido de la clave pública en el campo Contenido de la clave pública.
6. Elija Import key pair (Importar par de claves).
7. Compruebe que la clave pública importada aparezca en la lista de pares de claves.

AWS CLI

Para importar la clave pública a Amazon EC2

Utilice el comando de la AWS CLI import-key-pair:

Para comprobar que el par de claves se importó correctamente

Utilice el comando de la AWS CLI describe-key-pairs:

PowerShell

Para importar la clave pública a Amazon EC2

Utilice el comando de la AWS Tools for Windows PowerShell Import-EC2KeyPair:

Para comprobar que el par de claves se importó correctamente

Utilice el comando de la AWS Tools for Windows PowerShell Get-EC2KeyPair:

Etiquetar un par de claves

Para categorizar y administrar los pares de claves que ha creado con Amazon EC2 o ha importado a Amazon EC2, puede etiquetarlos con metadatos personalizados. Para obtener más información sobre cómo funcionan las etiquetas, consulte Etiquetar los recursos de Amazon EC2.

Console

Para ver, agregar o eliminar una etiqueta de un par de claves

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Pares de claves.
3. Seleccione una clave pública y, a continuación, elija Acciones, Administrar etiquetas.
4. La página Administrar etiquetas muestra las etiquetas asignadas a la clave pública.
   - Para agregar una etiqueta, elija Agregar etiqueta y, a continuación, escriba la clave y el valor de la etiqueta. Puede agregar hasta 50 etiquetas por clave. Para obtener más información, consulte Restricciones de las etiquetas.
   - Para eliminar una etiqueta, elija Eliminar junto a la etiqueta.
5. Seleccione Guardar.

AWS CLI

Para ver las etiquetas de los pares de claves

Utilice el comando de la AWS CLI describe-tags: En el siguiente ejemplo, se describen las etiquetas de todas las claves públicas.

```
aws ec2 describe-tags --filters "Name=resource-type,Values=key-pair"
```

```
{
    "Tags": [
    {
        "Key": "Environment",
        "ResourceId": "key-0123456789EXAMPLE",
        "ResourceType": "key-pair",
        "Value": "Production"
    },
    {
        "Key": "Environment",
        "ResourceId": "key-9876543210EXAMPLE",
        "ResourceType": "key-pair",
        "Value": "Production"
    }]
}
```

Para describir las etiquetas de un par de claves

Utilice el comando de la AWS CLI describe-key-pairs:

```
aws ec2 describe-key-pairs --key-pair-ids key-0123456789EXAMPLE
```

```
{
    "KeyPairs": [
    {
        "KeyName": "MyKeyPair",
        "KeyFingerprint":
 "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
        "KeyPairId": "key-0123456789EXAMPLE",
        "Tags": [
        {
            "Key": "Environment",
            "Value": "Production"
        }]
    }]
}
```

Para etiquetar un par de claves

Utilice el comando de la AWS CLI create-tags: En el siguiente ejemplo, la clave pública se etiqueta con `Key=Cost-Center` y `Value=CC-123`.

```
aws ec2 create-tags --resources key-0123456789EXAMPLE --tags Key=Cost-
Center,Value=CC-123
```

Para eliminar una etiqueta de un par de claves

Utilice el comando de la AWS CLI delete-tags: Para obtener ejemplos, consulte Ejemplos en la Referencia de comandos de la AWS CLI.

PowerShell

Para ver las etiquetas de los pares de claves

Utilice el comando Get-EC2Tag.

Para describir las etiquetas de un par de claves

Utilice el comando Get-EC2KeyPair.

Para etiquetar un par de claves

Utilice el comando New-EC2Tag.

Para eliminar una etiqueta de un par de claves

Utilice el comando Remove-EC2Tag.

Descripción de los pares de claves

Puede describir los pares de claves que se almacenan en Amazon EC2. También puede recuperar el material de la clave pública e identificar la clave pública que se especificó en el lanzamiento.

Temas

- Descripción de los pares de claves
- Recupere el material de la clave pública
- Identificación del par de claves públicas que se especificó en el lanzamiento

Descripción de los pares de claves

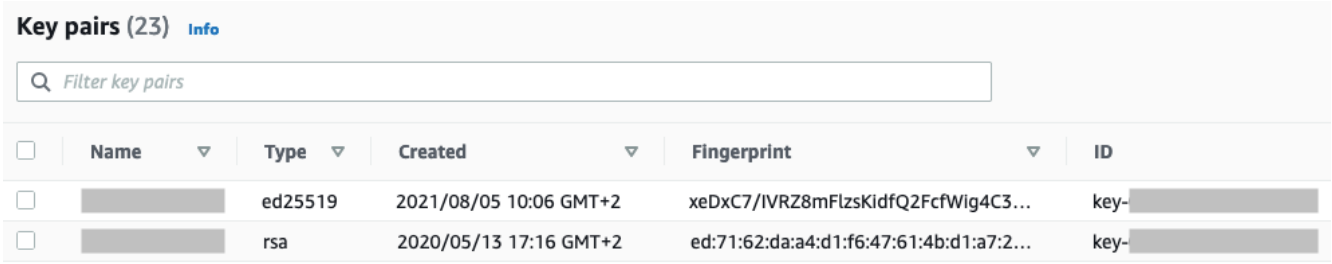
Puede ver la siguiente información sobre las claves públicas que se almacenan en Amazon EC2: nombre de clave pública, ID, tipo de clave, huella digital, material de clave pública, fecha y hora (en la zona horaria UTC) en que Amazon EC2 creó la clave (si la clave la creó una herramienta de terceros, entonces es la fecha y la hora en que la clave se importó a Amazon EC2) y cualquier etiqueta asociada a la clave pública.

Puede utilizar la consola de Amazon EC2 o la AWS CLI para ver información sobre las claves públicas.

Console

Para ver información sobre las claves públicas

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación izquierdo, elija Key Pairs (Par de claves).
3. Puede ver información sobre cada clave pública en la tabla Pares de claves.



4. Para ver las etiquetas de una clave pública, seleccione la casilla de verificación situada junto a la clave y, a continuación, elija Acciones, Administrar etiquetas.

AWS CLI

Para describir una clave pública

Utilice el comando describe-key-pairs y especifique el parámetro `--key-names`.

```
aws ec2 describe-key-pairs --key-names key-pair-name
```

Ejemplo de resultado

```
{
```

```
    "KeyPairs": [
        {
            "KeyPairId": "key-0123456789example",
            "KeyFingerprint":
 "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
            "KeyName": "key-pair-name",
            "KeyType": "rsa",
            "Tags": [],
            "CreateTime": "2022-04-28T11:37:26.000Z"
        }
    ]
}
```

También, en lugar de `--key-names`, puede especificar el parámetro `--key-pair-ids` para identificar la clave pública.

```
aws ec2 describe-key-pairs --key-pair-ids key-0123456789example
```

Para ver el material de clave pública en el resultado, debe especificar el parámetro `--include-public-key`.

```
aws ec2 describe-key-pairs --key-names key-pair-name --include-public-key
```

Resultado de ejemplo: en el resultado, el campo `PublicKey` contiene el material de clave pública.

```
{
    "KeyPairs": [
        {
            "KeyPairId": "key-0123456789example",
            "KeyFingerprint":
 "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
            "KeyName": "key-pair-name",
            "KeyType": "rsa",
            "Tags": [],
            "PublicKey": "ssh-ed25519
 AAAAC3NzaC1lZDI1NTE5AAAAIIj7azlDjVHAsSxgcpCRZ3oWnTm0nAFM64y9jd22ioI/ my-key-pair",
            "CreateTime": "2022-04-28T11:37:26.000Z"
        }
    ]
}
```

Recupere el material de la clave pública

Puede utilizar varios métodos para obtener acceso al material de clave pública. Puede recuperar el material de la clave pública de la clave privada correspondiente en su equipo local o de los metadatos de instancia en la instancia que se lanzó con la clave pública, o mediante el comando `describe-key-pairs` AWS CLI. En el caso de las instancias de Linux, el material de clave pública también se puede recuperar del archivo `authorized_keys` de la instancia.

Utilice uno de los siguientes métodos para recuperar el material de la clave pública.

instancias de Linux

From the private key

Para recuperar el material de la clave pública a partir de la clave privada

En su equipo Linux o macOS local, puede utilizar el comando ssh-keygen para recuperar la clave pública de su par de claves. Especifique la ruta donde descargó la clave privada (el archivo `.pem`).

```
ssh-keygen -y -f /path_to_key_pair/my-key-pair.pem
```

El comando devuelve la clave pública, como se muestra en el siguiente ejemplo.

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE
```

Si el comando produce un error, ejecute los siguientes comandos para asegurarse de que ha cambiado los permisos de su archivo de par de claves privadas para que solo usted pueda verlo.

```
chmod 400 key-pair-name.pem
```

From the instance metadata

Puede utilizar la versión 2 del servicio de metadatos de instancia o la versión 1 del servicio de metadatos de instancia a fin de recuperar la clave pública de los metadatos de la instancia.

> **Note**
>
> Si cambia el par de claves que utiliza para conectarse a la instancia, Amazon EC2 no actualiza los metadatos de la instancia para mostrar la nueva clave pública. Los metadatos de la instancia siguen mostrando la clave pública del par de claves que especificó al iniciar la instancia.

Para recuperar el material de la clave pública de los metadatos de la instancia

Utilice uno de los siguientes comandos de su instancia.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
```

Ejemplo de resultado

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE key-pair-name
```

Para obtener más información acerca de los metadatos de instancias, consulte Recuperar metadatos de instancia.

From the instance

Si especifica un par de claves al iniciar una instancia de Linux, cuando la instancia se arranca por primera vez, el contenido de la clave pública se coloca en la instancia en una entrada dentro de `~/.ssh/authorized_keys`.

Para recuperar el material de la clave pública de una instancia

1. Conéctese a la instancia.
2. En la ventana del terminal, abra el archivo `authorized_keys` con su editor de texto favorito (como vim o nano).

```
[ec2-user ~]$ nano ~/.ssh/authorized_keys
```

El archivo `authorized_keys` se abre y muestra la clave pública seguida del nombre del par de claves. A continuación se incluye una entrada de ejemplo para el par de claves llamado *key-pair-name*.

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE key-pair-name
```

From describe-key-pairs

Recuperar el material de la clave pública con el comando **`describe-key-pairs`**AWS CLI

Utilice el comando describe-key-pairs y especifique el parámetro `--key-names` para identificar la clave pública. Para incluir el material de clave pública en el resultado, especifique el parámetro `--include-public-key`.

```
aws ec2 describe-key-pairs --key-names key-pair-name --include-public-key
```

Resultado de ejemplo: en el resultado, el campo `PublicKey` contiene el material de clave pública.

```
{
    "KeyPairs": [
        {
            "KeyPairId": "key-0123456789example",
            "KeyFingerprint":
 "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
            "KeyName": "key-pair-name",
            "KeyType": "rsa",
```

```
            "Tags": [],
            "PublicKey": "ssh-ed25519
 AAAAC3NzaC1lZDI1NTE5AAAAIIj7azlDjVHAsSxgcpCRZ3oWnTm0nAFM64y9jd22ioI/ my-key-pair",
            "CreateTime": "2022-04-28T11:37:26.000Z"
        }
    ]
}
```

También, en lugar de `--key-names`, puede especificar el parámetro `--key-pair-ids` para identificar la clave pública.

```
aws ec2 describe-key-pairs --key-pair-ids key-0123456789example --include-public-key
```

instancias de Windows

From the private key

Para recuperar el material de la clave pública a partir de la clave privada

En su equipo Windows local puede utilizar PuTTYgen para obtener la clave pública para su par de claves.

Inicie PuTTYgen y elija Cargar. Seleccione el archivo `.ppk` o `.pem` de clave privada. PuTTYgen muestra la clave pública en Clave pública para pegar en el archivo authorized_keys de Open SSH. También puede ver la clave pública eligiendo Guardar clave pública, especificando un nombre para el archivo, guardando el archivo y abriendo después el archivo.

From the instance metadata

Puede utilizar la versión 2 del servicio de metadatos de instancia o la versión 1 del servicio de metadatos de instancia a fin de recuperar la clave pública de los metadatos de la instancia.

> **Note**
>
> Si cambia el par de claves que utiliza para conectarse a la instancia, Amazon EC2 no actualiza los metadatos de la instancia para mostrar la nueva clave pública. Los metadatos de la instancia siguen mostrando la clave pública del par de claves que especificó al iniciar la instancia.

Para recuperar el material de la clave pública de los metadatos de la instancia

Utilice uno de los siguientes comandos de su instancia.

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri  http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
```

Ejemplo de resultado

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE key-pair-name
```

Para obtener más información acerca de los metadatos de instancias, consulte Recuperar metadatos de instancia.

From describe-key-pairs

Recuperar el material de la clave pública con el comando **`describe-key-pairs`**AWS CLI

Utilice el comando describe-key-pairs y especifique el parámetro `--key-names` para identificar la clave pública. Para incluir el material de clave pública en el resultado, especifique el parámetro `--include-public-key`.

```
aws ec2 describe-key-pairs --key-names key-pair-name --include-public-key
```

Resultado de ejemplo: en el resultado, el campo `PublicKey` contiene el material de clave pública.

```
{
```

```
    "KeyPairs": [
        {
            "KeyPairId": "key-0123456789example",
            "KeyFingerprint":
 "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
            "KeyName": "key-pair-name",
            "KeyType": "rsa",
            "Tags": [],
            "PublicKey": "ssh-ed25519
 AAAAC3NzaC1lZDI1NTE5AAAAIIj7azlDjVHAsSxgcpCRZ3oWnTm0nAFM64y9jd22ioI/ my-key-pair",
            "CreateTime": "2022-04-28T11:37:26.000Z"
        }
    ]
}
```

También, en lugar de `--key-names`, puede especificar el parámetro `--key-pair-ids` para identificar la clave pública.

```
aws ec2 describe-key-pairs --key-pair-ids key-0123456789example --include-public-key
```

Identificación del par de claves públicas que se especificó en el lanzamiento

Si especifica una clave pública cuando lanza una instancia, la instancia registra el nombre de la clave pública.

Para identificar la clave pública que se especificó durante el lanzamiento

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instancias y seleccione la instancia.
3. En la pestaña Detalles, en Detalles de la instancia, el campo Par de claves asignadas en el lanzamiento muestra el nombre de la clave pública especificado al iniciar la instancia.

> **Note**
>
> El valor del campo Par de claves asignadas en el lanzamiento no cambia aunque cambie la clave pública de la instancia o se agreguen unas nuevas.

Eliminar un par de claves

Puede eliminar un par de claves, lo que elimina la clave pública que se almacena en Amazon EC2. La eliminación de un par de claves no elimina la clave privada correspondiente.

Cuando elimina una clave pública mediante los siguientes métodos, solo estará eliminando la clave pública que almacenó en Amazon EC2 en el momento de crear o importar el par de claves. La eliminación de una clave pública no la elimina de las instancias a las que la haya agregado, ya sea al iniciar la instancia o posteriormente. Tampoco elimina la clave privada guardada en su computadora local. Puede seguir conectándose a las instancias que haya lanzado mediante una clave pública que haya eliminado de Amazon EC2, siempre y cuando siga teniendo el archivo de clave privada (`.pem`).

> **Important**
>
> Si utiliza un grupo de Auto Scaling (por ejemplo, en un entorno de Elastic Beanstalk), asegúrese de que la clave pública que eliminará no se especifique en una plantilla de lanzamiento ni una configuración de lanzamiento asociadas. Si Amazon EC2 Auto Scaling detecta una instancia en mal estado, lanzará una instancia de reemplazo. Sin embargo, se producirá un error en el lanzamiento de la instancia si no se encuentra la clave pública. Para obtener más información, consulte Plantillas de lanzamiento en la Guía del usuario de Amazon EC2 Auto Scaling.

Console

Para eliminar la clave pública en Amazon EC2

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Pares de claves.
3. Seleccione el par de claves que desea eliminar y elija Acciones, Eliminar.
4. En el campo de confirmación, escriba `Delete` y, a continuación, elija Eliminar.

AWS CLI

Para eliminar la clave pública en Amazon EC2

Utilice el comando de la AWS CLI delete-key-pair:

PowerShell

Para eliminar la clave pública en Amazon EC2

Utilice el comando de la AWS Tools for Windows PowerShell Remove-EC2KeyPair:

Agregado o eliminación de una clave pública en su instancia de Linux

Si pierde una clave privada, perderá el acceso a todas las instancias que usen el par de claves. Para obtener más información sobre la conexión a una instancia mediante un par de claves diferente al que especificó en el lanzamiento, consulte Perdí mi clave privada.

Al lanzar una instancia, puede especificar el par de claves. Si especifica un par de claves durante el lanzamiento, cuando la instancia se arranca por primera vez, el material de la clave pública se coloca en la instancia de Linux en una entrada dentro de `~/.ssh/authorized_keys`.

Puede cambiar el par de claves que se utiliza para acceder a la cuenta predeterminada del sistema de la instancia agregando una nueva clave pública en la instancia o reemplazando la clave pública (es decir, eliminando la clave pública existente y agregando una nueva) en la instancia. También puede eliminar todas las claves públicas de una instancia. Para añadir o reemplazar un par de claves, tiene que conectarse a su instancia.

Puede agregar o sustituir un par de claves por los motivos siguientes:

- Si un usuario de su organización tiene que acceder al usuario del sistema con un par de claves diferente, puede agregar la clave pública a la instancia.
- Si alguien tiene una copia de la clave privada (archivo `.pem`) y usted quiere evitar que se conecte a la instancia (en caso de que, por ejemplo, ya no pertenezca a la organización), puede eliminar la clave pública de la instancia y reemplazarla por una nueva.
- Si crea una AMI de Linux a partir de una instancia, el material de la clave pública se copia de la instancia a la AMI. Si lanza una instancia a partir de la AMI, la nueva instancia incluirá la clave pública de la instancia original. Para evitar que alguien que tenga la clave privada se conecte a la nueva instancia, puede eliminar la clave pública de la instancia original antes de crear la AMI.

Utilice los procedimientos siguientes para modificar el par de claves para el usuario predeterminado como, por ejemplo, `ec2-user`. Para obtener información sobre cómo agregar usuarios a la instancia, consulte la documentación del sistema operativo de la instancia.

Para agregar o sustituir un par de claves

1. Cree un nuevo par de claves mediante la consola de Amazon EC2 o una herramienta de terceros.
2. Recupere la clave pública a partir de su nuevo par de claves. Para obtener más información, consulte Recupere el material de la clave pública.
3. Conéctese a la instancia con la clave privada existente.
4. Con el editor de texto que desee, abra el archivo `.ssh/authorized_keys` en la instancia. Pegue la información de la clave pública de su nuevo par de claves debajo de la información de la clave pública existente. Guarde el archivo.
5. Desconéctese de la instancia y compruebe que puede volver a conectarse a la instancia utilizando el nuevo archivo de clave privada.
6. (Opcional) Si desea sustituir un par de claves existente, conéctese a la instancia y elimine la información de la clave pública para el par de claves original del archivo `.ssh/authorized_keys`.

> **Important**
>
> Si utiliza un grupo de Auto Scaling, asegúrese de que el par de claves que va a reemplazar no se especifique en la plantilla de lanzamiento ni en la configuración de lanzamiento. Si Amazon EC2 Auto Scaling detecta una instancia en mal estado, lanzará una instancia de reemplazo. Sin embargo, el lanzamiento de la instancia fallará si no se encuentra el par de claves. Para obtener más información, consulte Plantillas de lanzamiento en la Guía del usuario de Amazon EC2 Auto Scaling.

Para eliminar la clave pública de una instancia

1. Conéctese a la instancia.
2. Con el editor de texto que desee, abra el archivo `.ssh/authorized_keys` en la instancia. Elimine la información de la clave pública y, a continuación, guarde el archivo.

> **Warning**
>
> Después de eliminar todas las claves públicas de una instancia y desconectarse de ella, no podrá volver a conectarse a ella, a menos que la AMI proporcione otra forma de iniciar sesión.

Verificar la huella digital de su par de claves

Para comprobar la huella digital de su par de claves, compare la huella digital que aparece en la página Pares de claves de la consola de Amazon EC2, o la que devuelve el comando describe-key-pairs, con la huella digital que genere con la clave privada de su equipo local. Estas huellas digitales deben coincidir.

Cuando Amazon EC2 calcula una huella digital, Amazon EC2 puede añadir un relleno a la huella digital con caracteres =. Otras herramientas, como ssh-keygen, pueden omitir este relleno.

Si está intentando verificar la huella digital de su instancia de Linux EC2, y no la huella digital de su par de claves, consulte Obtener la huella digital de la instancia.

Cómo se calculan las huellas digitales

Amazon EC2 utiliza diferentes funciones hash para calcular las huellas digitales de los pares de claves RSA y ED25519. Además, en el caso de los pares de claves RSA, Amazon EC2 calcula las huellas digitales de forma diferente con distintas funciones hash, según si el par de claves lo ha creado Amazon EC2 o se ha importado en Amazon EC2.

En la tabla siguiente aparecen las funciones hash que se utilizan para calcular las huellas digitales de los pares de claves RSA y ED25519 que crea Amazon EC2 y se importan en Amazon EC2.

(Instancias de Linux) Funciones hash utilizadas para calcular la huella digital

Origen de par de claves	Pares de claves RSA (Windows y Linux)	Pares de claves ED25519 (Linux)
Creados por Amazon EC2	SHA-1	SHA-256
Importados en Amazon EC2	MD5[1]	SHA-256

[1] Si importa una clave RSA pública en Amazon EC2, la huella digital se calcula mediante una función hash MD5. Esto es así con independencia de cómo haya creado el par de claves; por ejemplo, mediante una herramienta de terceros, o bien generando una nueva clave pública a partir de una clave privada existente creada con Amazon EC2.

Cuando se utiliza el mismo par de claves en distintas regiones

Si tiene previsto utilizar el mismo par de claves para conectarse a instancias de distintas Regiones de AWS, debe importar la clave pública en todas las regiones en las que vaya a utilizarla. Si utiliza Amazon EC2 para crear el par de claves, Recupere el material de la clave pública para poder importar la clave pública en las demás regiones.

> **Note**
>
> - Si crea un par de claves RSA con Amazon EC2 y luego genera una clave pública a partir de la clave privada de Amazon EC2, las claves públicas importadas tendrán una huella digital diferente a la de la clave pública original. Esto se debe a que la huella digital de la clave RSA original creada con Amazon EC2 se calcula mediante una función hash SHA-1, mientras que la huella digital de las claves RSA importadas se calcula mediante una función hash MD5.
> - En el caso de los pares de claves ED25519, las huellas digitales serán iguales, con independencia de si las ha creado Amazon EC2 o se han importado en Amazon EC2, porque se utiliza la misma función hash SHA-256 para calcularlas.

Generar una huella digital a partir de la clave privada

Utilice uno de los siguientes comandos para generar una huella digital a partir de la clave privada de la máquina local.

Si utiliza un equipo local de Windows, puede ejecutar los siguientes comandos utilizando Windows Subsystem for Linux (WSL). Instale el WSL y una distribución de Linux utilizando las instrucciones de la Guía de instalación de Windows 10. El ejemplo que aparece en las instrucciones instala la distribución Ubuntu de Linux, pero puede instalar cualquier distribución. Se le solicita que reinicie su equipo para que se apliquen los cambios.

- Si ha creado el par de claves con Amazon EC2

Utilice las herramientas de OpenSSL para generar una huella digital como se muestra en los siguientes ejemplos.

Para pares de claves RSA:

```
openssl pkcs8 -in path_to_private_key -inform PEM -outform DER -topk8 -nocrypt |
 openssl sha1 -c
```

(Instancias de Linux) Para pares de claves ED25519:

```
ssh-keygen -l -f path_to_private_key
```

- (Solo pares de claves RSA): si ha importado la clave pública a Amazon EC2

  Puede seguir este procedimiento independientemente de cómo haya creado el par de claves; por ejemplo, mediante una herramienta de terceros o bien al generar una nueva clave pública a partir de una clave privada existente creada con Amazon EC2.

  Utilice las herramientas de OpenSSL para generar la huella digital como se muestra en el siguiente ejemplo.

  ```
  openssl rsa -in path_to_private_key -pubout -outform DER | openssl md5 -c
  ```

- Si ha creado un par de claves OpenSSH con OpenSSH 7.8 o posterior y ha importado la clave pública en Amazon EC2

  Utilice ssh-keygen para generar la huella digital como se muestra en los siguientes ejemplos.

  Para pares de claves RSA:

  ```
  ssh-keygen -ef path_to_private_key -m PEM | openssl rsa -RSAPublicKey_in -outform DER
   | openssl md5 -c
  ```

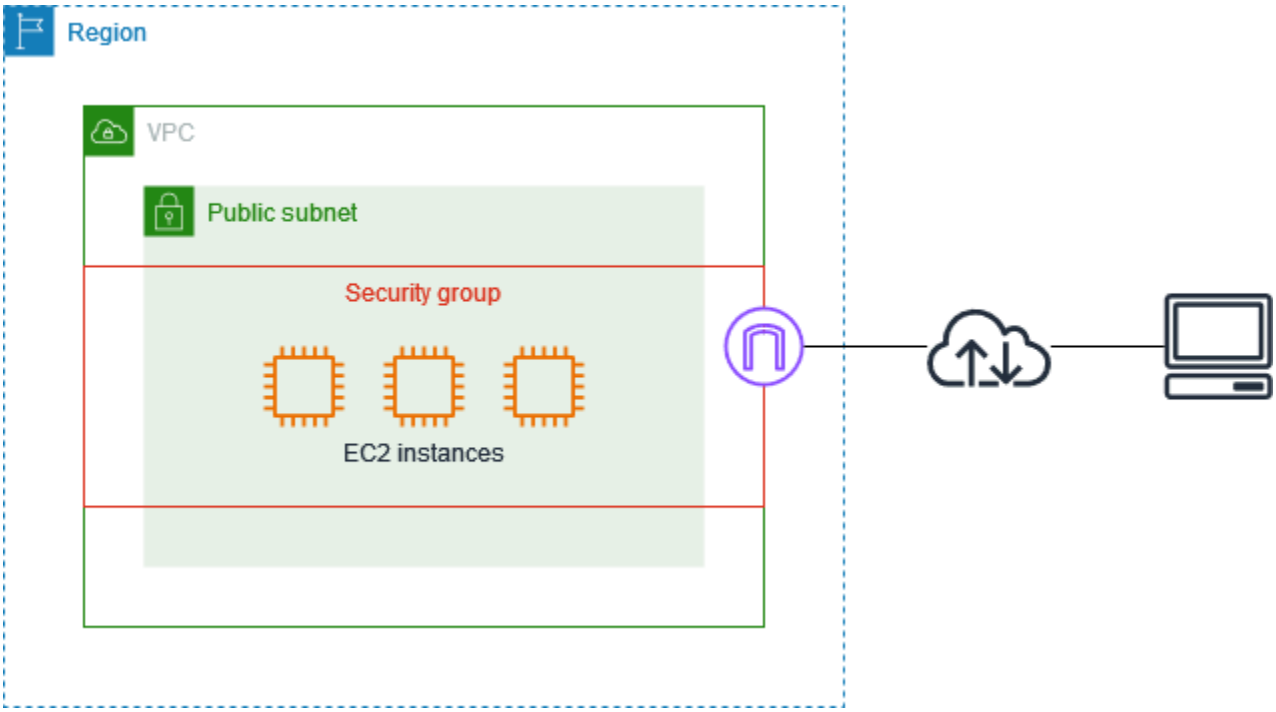
  (Instancias de Linux) Para pares de claves ED25519:

  ```
  ssh-keygen -l -f path_to_private_key
  ```

Grupos de seguridad de Amazon EC2 para instancias EC2

Un grupo de seguridad funciona como un firewall virtual para las instancias de EC2 para controlar el tráfico entrante y saliente. Las reglas de entrada controlan el tráfico entrante a la instancia y las reglas de salida controlan el tráfico saliente desde la instancia. Al iniciar una instancia puede especificar uno o varios grupos de seguridad. Si no especifica un grupo de seguridad, Amazon EC2 utiliza el grupo de seguridad predeterminado para la VPC. Puede añadir reglas a cada grupo de seguridad que permitan el tráfico a o desde sus instancias asociadas. Puede modificar las reglas de un grupo de seguridad en cualquier momento. Las reglas nuevas y modificadas se aplican automáticamente a todas las instancias asociadas al grupo de seguridad. Cuando Amazon EC2 decide si se permite que el tráfico llegue a una instancia, evalúa todas las reglas de todos los grupos de seguridad asociados a la instancia.

En el siguiente diagrama se muestra una VPC con una subred, una puerta de enlace de Internet y un grupo de seguridad. La subred contiene instancias de EC2. El grupo de seguridad se asigna a estas. El único tráfico que llega a la instancia es el permitido por las reglas del grupo de seguridad. Por ejemplo, si el grupo de seguridad contiene una regla que permite el tráfico SSH a la instancia desde su red, puede conectarse a la instancia desde su equipo mediante SSH. Si el grupo de seguridad contiene una regla que permite todo el tráfico de los recursos que se le han asignado, cada instancia puede recibir el tráfico que se envía desde las demás instancias.



Una vez lanzada la instancia, puede cambiar sus grupos de seguridad. Los grupos de seguridad están asociados a interfaces de red. Al cambiar los grupos de seguridad de una instancia se cambian los grupos de seguridad asociados a la interfaz de red principal (eth0). Para obtener más información, consulte Cambiar el grupo de seguridad de una instancia. También puede cambiar los grupos de seguridad asociados a cualquier otra interfaz de red. Para obtener más información, consulte Modificar atributos de interfaz de red.

La seguridad es una responsabilidad compartida entre AWS y usted. Para más información, consulte Seguridad en Amazon EC2. AWS proporciona grupos de seguridad como una de las herramientas para proteger las instancias y debe configurarlos para satisfacer sus necesidades de seguridad. Si tiene requisitos que no cumplen totalmente los grupos de seguridad, puede mantener su propio firewall en cualquiera de las instancias, además de usar grupos de seguridad.

El uso de grupos de seguridad no supone ningún cargo adicional.

Contenido

Reglas del grupo de seguridad

Las reglas de un grupo de seguridad controlan el tráfico entrante que puede llegar a las instancias asociadas al grupo de seguridad. Las reglas también controlan el tráfico saliente que puede salir de ellos.

A continuación, se describen las características de las reglas de los grupos de seguridad:

- Los grupos de seguridad incluyen de forma predeterminada reglas de salida que permiten todo el tráfico saliente. Puede eliminar estas reglas. Tenga en cuenta que Amazon EC2 bloquea el tráfico en el puerto 25 de forma predeterminada. Para obtener más información, consulte Restricción en el correo electrónico enviado a través del puerto 25.
- Las reglas del grupo de seguridad son siempre permisivas; no puede crear reglas que denieguen el acceso.

- Las reglas de grupo de seguridad le permiten filtrar el tráfico en función de los protocolos y números de puerto.
- Los grupos de seguridad tienen estado: si envía una solicitud desde su instancia, se permite el flujo del tráfico de respuesta para dicha solicitud independientemente de las reglas de entrada del grupo de seguridad. En los grupos de seguridad de VPC, esto significa también que el flujo de salida de las respuestas al tráfico de entrada está permitido, independientemente de las reglas de salida. Para obtener más información, consulte Seguimiento de conexiones de grupos de seguridad.
- Puede agregar y eliminar reglas en cualquier momento. Los cambios se aplican automáticamente a las instancias que están asociadas al grupo de seguridad.

  El efecto de algunos cambios en las reglas puede depender de cómo se realiza el seguimiento del tráfico. Para obtener más información, consulte Seguimiento de conexiones de grupos de seguridad.
- Al asociar varios grupos de seguridad a una instancia, las reglas de cada grupo de seguridad se agregan de manera eficiente para crear un conjunto de reglas. Amazon EC2 utiliza este conjunto de reglas para determinar si permite o no el acceso.

  Puede asignar varios grupos de seguridad a una instancia. Por lo tanto, una instancia puede tener cientos de reglas que se aplican. Esto puede causar problemas al obtener acceso a la instancia. Le recomendamos que condense las reglas en la medida de lo posible.

> **Note**
>
> Los grupos de seguridad no pueden bloquear las solicitudes de DNS hacia el servicio Route 53 Resolver o desde el mismo, a veces denominado “dirección IP de VPC+2” (consulte ¿Qué es Amazon Route 53 Resolver? en la Guía para desarrolladores de Amazon Route 53) o “AmazonProvidedDNS” (consulte Trabajo con conjuntos de opciones de DHCP en la Guía del usuario de Amazon Virtual Private Cloud). Si desea filtrar las solicitudes de DNS a través de Route 53 Resolver, puede habilitar el firewall de DNS de Route 53 Resolver (consulte Firewall de DNS de Route 53 Resolver en la Guía para desarrolladores de Amazon Route 53).

Especifique lo siguiente para cada regla:

- Nombre: el nombre del grupo de seguridad (por ejemplo, “my-security-group”).

Un nombre puede tener hasta 255 caracteres como máximo. Los caracteres permitidos incluyen a-z, A-Z, 0-9, espacios y ._-:/()#,@[]+=;{}!$*. Si el nombre contiene espacios finales, se eliminan al guardarlo. Por ejemplo, si introduce el nombre "Grupo de seguridad de prueba ", se guardará como "Grupo de seguridad de prueba".

- Protocolo: el protocolo que se permite. Los protocolos más habituales son 6 (TCP), 17 (UDP) y 1 (ICMP).
- Rango de puertos: para TCP, UDP o un protocolo personalizado, el rango de puertos que se permite. Puede especificar un solo número de puerto (por ejemplo, 22), o bien un rango de números de puertos (por ejemplo, `7000-8000`).
- Tipo y código ICMP: para ICMP, el tipo y el código ICMP. Por ejemplo, utilice el tipo 8 para la Echo Request de ICMP o el tipo 128 para la Echo Request de ICMPv6.
- Origen o destino: el origen (reglas de entrada) o el destino (reglas de salida) del tráfico que se va a permitir. Especifique uno de los siguientes valores:
  - Una única dirección IPv4. Debe utilizar la longitud de prefijo `/32`. Por ejemplo, `203.0.113.1/32`.
  - Una única dirección IPv6. Debe utilizar la longitud de prefijo `/128`. Por ejemplo, `2001:db8:1234:1a00::123/128`.
  - Un rango de direcciones IPv4 en notación de bloque de CIDR. Por ejemplo, `203.0.113.0/24`.
  - Un rango de direcciones IPv6 en notación de bloque de CIDR. Por ejemplo, `2001:db8:1234:1a00::/64`.
  - El ID de una lista de prefijos. Por ejemplo, `pl-1234abc1234abc123`. Para obtener más información, consulte Listas de prefijos en la Guía del usuario de Amazon VPC.
  - El ID de un grupo de seguridad (al que se hace referencia aquí como el grupo de seguridad especificado). Por ejemplo, el grupo de seguridad actual, un grupo de seguridad de la misma VPC o un grupo de seguridad para una VPC interconectada. Esto permite el tráfico en función de las direcciones IP privadas de los recursos asociados al grupo de seguridad especificado. Esto no agrega reglas del grupo de seguridad especificado al grupo de seguridad actual.
- (Opcional) Descripción: puede agregar una descripción a la regla, que puede ayudarlo a identificarla más adelante. Una descripción puede tener una longitud máxima de 255 caracteres. Los caracteres permitidos incluyen a-z, A-Z, 0-9, espacios y ._-:/()#,@[]+=;{}!$*.

Cuando usted crea una regla de grupo de seguridad, AWS le asigna un ID único. Puede utilizar el ID de una regla cuando utilice la API o la CLI para modificarla o eliminarla.

Al especificar un grupo de seguridad como origen o destino de una regla, la regla afecta a todas las instancias que están asociadas al grupo de seguridad. Se permite el tráfico entrante según las direcciones IP privadas de las instancias asociadas al grupo de seguridad de origen (y no la dirección IP pública o las direcciones IP elásticas). Para obtener más información acerca de las direcciones IP, consulte Direccionamiento IP de instancias Amazon EC2. Si la regla de su grupo de seguridad hace referencia a un grupo de seguridad eliminado en la misma VPC o en una VPC del mismo nivel, o que hace referencia a un grupo de seguridad en una VPC del mismo nivel para la que se ha eliminado la conexión de emparejamiento de VPC, la regla se marca como obsoleta. Para obtener más información, consulte Uso de reglas de grupo de seguridad obsoletas en la Amazon VPC Peering Guide.

Si hay más de una regla para un puerto específico, Amazon EC2 aplica la regla más permisiva. Por ejemplo, si cuenta con una regla que permite el acceso al puerto TCP 22 (SSH) desde la dirección IP 203.0.113.1 y otra regla que permite el acceso al puerto TCP 22 desde todas las direcciones, todos tienen acceso al puerto TCP 22.

Si se agregan, actualizan o eliminan reglas, los cambios se aplican automáticamente a todas las instancias asociadas al grupo de seguridad.

Seguimiento de conexiones de grupos de seguridad

Los grupos de seguridad utilizan el seguimiento de las conexiones para realizar un seguimiento de la información sobre el tráfico hacia y desde la instancia. Las reglas se aplican según el estado de la conexión del tráfico para determinar si el tráfico se permite o se deniega. Con este enfoque, los grupos de seguridad tienen estado. Esto significa que se permite la salida de las repuestas al tráfico de entrada de la instancia, independientemente de las reglas de salida del grupo de seguridad y viceversa.

Por ejemplo, suponga que inicia un comando como netcat o alguno similar en las instancias desde la computadora doméstica y las reglas de tráfico de entrada del grupo de seguridad permiten el tráfico de ICMP. Se realiza un seguimiento de la información sobre la conexión (incluida la información del puerto). El tráfico de respuesta desde la instancia del comando no se sigue como una nueva solicitud, sino como una conexión establecida, y se permite que salga de la instancia, aunque las reglas de salida del grupo de seguridad restrinjan el tráfico de ICMP de salida.

En el caso de otros protocolos que no sean TCP, UDP o ICMP, solo se realiza el seguimiento de la dirección IP y del número de protocolo. Si la instancia envía tráfico a otro host, y este envía el mismo tipo de tráfico a su instancia en un plazo de 600 segundos, el grupo de seguridad de la instancia lo

acepta independientemente de las reglas de entrada. El grupo de seguridad lo acepta porque se considera un tráfico de respuesta del tráfico original.

Cuando cambia una regla del grupo de seguridad, las conexiones de seguimiento no se interrumpen de forma inmediata. El grupo de seguridad sigue permitiendo paquetes hasta que las conexiones existentes se agoten. Para asegurarse de que el tráfico se interrumpa de forma inmediata, o que todo el tráfico esté sujeto a reglas de firewall, independientemente del estado de seguimiento, puede utilizar una ACL de red para su subred. Las ACL de red son sin estado y, por lo tanto, no permiten automáticamente el tráfico de respuesta. Agregar una ACL de red que bloquee el tráfico en cualquier dirección provoca la interrupción de las conexiones existentes. Para obtener más información, consulte la sección relacionada con las ACL de red en la Guía del usuario de Amazon VPC.

> **Note**
>
> Los grupos de seguridad no afectan al tráfico de DNS hacia el servicio Route 53 Resolver o desde el mismo, a veces denominado “dirección IP de VPC+2” (consulte ¿Qué es Amazon Route 53 Resolver? en la Guía para desarrolladores de Amazon Route 53) o “AmazonProvidedDNS” (consulte Trabajo con conjuntos de opciones de DHCP en la Guía del usuario de Amazon Virtual Private Cloud). Si desea filtrar las solicitudes de DNS a través de Route 53 Resolver, puede habilitar el firewall de DNS de Route 53 Resolver (consulte Firewall de DNS de Route 53 Resolver en la Guía para desarrolladores de Amazon Route 53).

Conexiones sin seguimiento

No se realiza un seguimiento de todos los flujos de tráfico. Si una regla del grupo de seguridad permite los flujos TCP o UDP para todo el tráfico (0.0.0.0/0 o ::/0) y hay una regla correspondiente en la otra dirección que permita todo el tráfico de respuesta (0.0.0.0/0 o ::/0) para todos los puertos (0-65 535), no se realizará un seguimiento de ese flujo de tráfico, a menos que sea parte de una conexión de la cual se realiza un seguimiento de manera automática. En el caso de un flujo sin seguimiento, se permite el tráfico de respuesta en función de la regla de entrada o de salida que permita el tráfico de respuesta y no según la información de seguimiento.

Un flujo de tráfico del que no se realiza seguimiento se interrumpe de inmediato si se elimina o modifica la regla que permite el flujo. Por ejemplo, si tiene una regla de salida abierta (0.0.0.0/0) y elimina una regla que permite todo el tráfico SSH (puerto TCP 22) entrante (0.0.0.0/0) a la instancia (o la modifica de modo que la conexión ya no se permita), las conexiones SSH existentes a la

instancia se eliminan inmediatamente. La conexión no estaba siendo rastreada previamente, por lo que el cambio romperá la conexión. Por otro lado, si tiene una regla de entrada más estrecha que inicialmente permite la conexión SSH (lo que significa que se hizo un seguimiento de la conexión), pero cambia esa regla para que ya no permita nuevas conexiones desde la dirección del cliente SSH actual, la conexión SSH existente no se interrumpirá porque se le ha hecho un seguimiento.

Conexiones con seguimiento automático

Se hace un seguimiento automático de las conexiones realizadas a través de lo siguiente, incluso si la configuración del grupo de seguridad no requiere ningún tipo de seguimiento:

- Puerta de enlace de Internet de solo salida
- Aceleradores de Global Accelerator
- Puerta de enlace de NAT
- Puntos de conexión de firewall de Network Firewall
- Equilibrador de carga de red
- AWS PrivateLink (Puntos de conexión de VPC de tipo interfaz)
- AWS Lambda (interfaces de red elásticas de hiperplano)

Permisos de seguimiento de conexiones

Amazon EC2 define el número máximo de conexiones que se pueden rastrear por instancia. Una vez alcanzado el máximo, los paquetes que se envían o reciben se pierden porque no se puede establecer una nueva conexión. Cuando esto sucede, las aplicaciones que envían y reciben paquetes no pueden comunicarse correctamente. Utilice la métrica de rendimiento de red `conntrack_allowance_available` para determinar la cantidad de conexiones rastreadas que aún están disponibles para ese tipo de instancia.

Para determinar si los paquetes se descartaron porque el tráfico de red de la instancia excedió el número máximo de conexiones que se pueden rastrear, utilice la métrica de rendimiento de red `conntrack_allowance_exceeded`. Para obtener más información, consulte Monitoreo del rendimiento de la red de la instancia de EC2.

Con Elastic Load Balancing, si supera el número máximo de conexiones que se pueden rastrear por instancia, se recomienda escalar el número de instancias registradas con el equilibrador de carga o el tamaño de instancias registradas con el equilibrador de carga.

Consideraciones sobre el rendimiento del seguimiento de conexiones

El enrutamiento asimétrico, en el que el tráfico entra en una instancia a través de una interfaz de red y sale por una interfaz de red diferente, puede reducir el rendimiento máximo que puede alcanzar una instancia si se realiza un seguimiento de los flujos.

Para mantener un rendimiento máximo cuando el seguimiento de conexiones está habilitado para sus grupos de seguridad, le recomendamos la siguiente configuración:

- Si es posible, evite las topologías de enrutamiento asimétrico.
- En lugar de usar grupos de seguridad para filtrar, utilice las ACL de la red.
- Si debe usar grupos de seguridad con seguimiento de conexiones, configure el tiempo de espera de conexión más corto posible.

Para obtener más información sobre el ajuste del rendimiento en el sistema Nitro, consulte Consideraciones sobre el Nitro System para ajustar el rendimiento.

Tiempo de espera de seguimiento de conexiones inactivas

El grupo de seguridad hace el seguimiento de cada conexión establecida para asegurarse de que los paquetes devueltos se entreguen como se espera. Existe un número máximo de conexiones que se pueden rastrear por instancia. Las conexiones que permanecen inactivas pueden provocar que se agote el seguimiento de las conexiones, que no se rastreen y que se pierdan paquetes. Puede establecer el tiempo de espera para el seguimiento de las conexiones inactivas en una interfaz de red elástica.

> **Note**
>
> Esta característica solo está disponible para las instancias integradas en el AWS Nitro System.

Hay tres tiempos de espera configurables:

- Tiempo de espera establecido de TCP: tiempo de espera (en segundos) para las conexiones TCP inactivas en un estado establecido. Valor mínimo: 60 segundos. Valor máximo: 432 000 segundos (5 días). Valor predeterminado: 432 000 segundos. Valor recomendado: menos de 432 000 segundos.

- Tiempo de espera de UDP: tiempo de espera (en segundos) para los flujos de UDP inactivos que solo han registrado tráfico en una sola dirección o en una sola transacción de solicitud-respuesta. Valor mínimo: 30 segundos. Valor máximo: 60 segundos. Valor predeterminado: 30 segundos.
- Tiempo de espera del flujo de UDP: tiempo de espera (en segundos) para los flujos de UDP inactivos clasificados como flujos que han recibido más de una transacción de solicitud-respuesta. Valor mínimo: 60 segundos. Valor máximo: 180 segundos (3 minutos). Valor predeterminado: 180 segundos.

Si quiere modificar los tiempos de espera predeterminados para cualquiera de los siguientes casos:

- Si supervisa las conexiones rastreadas mediante métricas de rendimiento de red de Amazon EC2, las métricas conntrack_allowance_exceeded y conntrack_allowance_available le permiten supervisar los paquetes descartados y el uso de las conexiones rastreadas para administrar de forma proactiva la capacidad de la instancia de EC2 con acciones de escalado vertical u horizontal para ayudar a satisfacer la demanda de conexiones de red antes de descartar paquetes. Si observa caídas de conntrack_allowance_exceeded en sus instancias de EC2, puede resultarle útil definir un tiempo de espera establecido de TCP más bajo para tener en cuenta las sesiones de TCP/UDP obsoletas que se deben a clientes o cajas intermedias de red inadecuadas.
- Por lo general, los equilibradores de carga o los firewalls tienen un tiempo de espera de inactividad establecido de TCP de entre 60 y 90 minutos. Si ejecuta cargas de trabajo que se espera que gestionen un número muy elevado de conexiones (más de 100 000) desde dispositivos como firewalls de red, se recomienda configurar un tiempo de espera similar en una interfaz de red de EC2.
- Si ejecuta una carga de trabajo que utiliza una topología de enrutamiento asimétrico, le recomendamos que configure un tiempo de espera de inactividad establecido de TCP de 60 segundos.
- Si ejecuta cargas de trabajo con un gran número de conexiones, como DNS, SIP, SNMP, Syslog, Radius y otros servicios que utilizan principalmente UDP para atender las solicitudes, establecer el tiempo de espera de “flujo de UDP” en 60 segundos proporciona una mayor escala o un mayor rendimiento para la capacidad existente y evita errores grises.
- En el caso de las conexiones TCP o UDP a través de equilibradores de carga de red (NLB) y equilibradores de carga elásticos (ELB), se hace un seguimiento de todas las conexiones. El valor de tiempo de espera de inactividad para los flujos de TCP es de 350 segundos y para los flujos de UDP es de 120 segundos, y varía según los valores de tiempo de espera de nivel de interfaz. Es posible que quiera configurar los tiempos de espera en el nivel de interfaz de red para permitir una

mayor flexibilidad de tiempo de espera que los tiempos de espera predeterminados para ELB o NLB.

Tiene la opción de configurar los tiempos de espera de seguimiento de conexiones si hace lo siguiente:

- Crear una interfaz de red
- Modificar atributos de interfaz de red
- Iniciar una instancia de EC2
- Crear una plantilla de lanzamiento de una instancia de EC2

Ejemplo

En el siguiente ejemplo, el grupo de seguridad incluye reglas de entrada que permiten el tráfico TCP e ICMP y reglas de salida que permiten todo el tráfico de salida.

Entrada

Tipo de protocolo	Número de puerto	Origen
TCP	22 (SSH)	203.0.113.1/32
TCP	80 (HTTP)	0.0.0.0/0
TCP	80 (HTTP)	::/0
ICMP	Todos	0.0.0.0/0

Salida

Tipo de protocolo	Número de puerto	Destino
Todos	Todos	0.0.0.0/0
Todos	Todos	::/0

Con una conexión de red directa a la instancia o la interfaz de red, el comportamiento del seguimiento es el siguiente:

- Se hace un seguimiento del tráfico TCP entrante y saliente en el puerto 22 (SSH), ya que la regla de entrada solo permite el tráfico desde 203.0.113.1/32 y no todas las direcciones IP (0.0.0.0/0).
- No se hace un seguimiento del tráfico TCP entrante y saliente en el puerto 80 (HTTP), ya que tanto las reglas de entrada como las de salida permiten el tráfico desde todas las direcciones IP.
- Siempre se hace un seguimiento del tráfico ICMP.

Si elimina la regla de salida para el tráfico IPv4, se hace un seguimiento de todo el tráfico IPv4 entrante y saliente, incluido el tráfico del puerto 80 (HTTP). Lo mismo ocurre con el tráfico IPv6 si se elimina la regla de salida para este.

Grupos de seguridad predeterminados y personalizados

La cuenta de AWS tiene automáticamente un grupo de seguridad predeterminado para la VPC predeterminada en cada región. Si no especifica ningún grupo de seguridad al iniciar una instancia, esta se asocia automáticamente al grupo de seguridad predeterminado de la VPC. Si no desea que las instancias usen el grupo de seguridad predeterminado, puede crear sus propios grupos de seguridad personalizados y especificarlos al iniciar las instancias.

Contenido

Grupos de seguridad predeterminados

Todas las VPC incluyen un grupo de seguridad predeterminado. Se recomienda crear grupos de seguridad para instancias o grupos de instancias específicos en lugar de utilizar el grupo de seguridad predeterminado. Por ejemplo, si no especifica ningún grupo de seguridad cuando lanza una instancia, la instancia se asocia al grupo de seguridad predeterminado para la VPC.

El nombre de un grupo de seguridad predeterminado es “default”. A continuación, se describen las reglas predeterminadas de cada grupo de seguridad predeterminado:

Entrada

Fuente	Protocolo	Rango de puerto	Descripción
sg-1234567890abcdef0	Todos	Todos	Permite el tráfico entrante de todos los recursos asignados a este grupo de seguridad. El origen es el ID de este grupo de seguridad.

Salida

Destino	Protocolo	Rango de puerto	Descripción
0.0.0.0/0	Todos	Todos	Permite todo el tráfico IPv4 saliente.
::/0	Todos	Todos	Permite todo el tráfico IPv6 saliente. Esta regla se agrega solo si su VPC tiene un bloque de CIDR IPv6 asociado.

Conceptos básicos de un grupo de seguridad predeterminado

- Puede cambiar las reglas de un grupo de seguridad predeterminado.
- El grupo de seguridad predeterminado no se puede eliminar. Si intenta eliminar el grupo de seguridad predeterminado, devolveremos el siguiente código de error: `Client.CannotDelete`.

Grupos de seguridad personalizados

Puede crear varios grupos de seguridad para reflejar los distintos roles de sus instancias, por ejemplo, servidores web o servidores de bases de datos.

Al crear un grupo de seguridad, debe darle un nombre y una descripción. Los nombres y las descripciones de los grupos de seguridad pueden tener hasta 255 caracteres de longitud y se limitan a los siguientes caracteres:

a-z, A-Z, 0-9, espacios y ._-:/()#,@[]+=&;{}!$*

El nombre del grupo de seguridad no puede comenzar con sg-. El nombre de un grupo de seguridad debe ser único en la VPC.

A continuación, se describen las reglas predeterminadas de un grupo de seguridad que crea:

- No permite ningún tráfico de entrada
- Permite todo el tráfico de salida

Una vez que ha creado un grupo de seguridad, puede cambiar las reglas de entrada para que reflejen el tipo de tráfico de entrada que desea que llegue a las instancias asociadas. También puede cambiar sus reglas de salida.

Para obtener más información sobre las reglas que puede añadir a un grupo de seguridad, consulte Reglas de grupo de seguridad para diferentes casos de uso.

Trabajar con grupos de seguridad

Puede asignar un grupo de seguridad a una instancia al lanzar la instancia. Al añadir o quitar reglas, esos cambios se aplican automáticamente a todas las instancias a las que ha asignado el grupo de seguridad. Para obtener más información, consulte Asignar un grupo de seguridad a una instancia.

Una vez lanzada la instancia, puede cambiar sus grupos de seguridad. Para obtener más información, consulte Cambiar el grupo de seguridad de una instancia.

Puede crear, ver, actualizar y eliminar grupos de seguridad y las reglas de los grupos de seguridad mediante la consola de Amazon EC2 y las herramientas de la línea de comandos.

Tareas

- Crear un grupo de seguridad
- Copiar un grupo de seguridad
- Ver los grupos de seguridad
- Agregar reglas a un grupo de seguridad
- Actualizar reglas de los grupos de seguridad
- Eliminar reglas de un grupo de seguridad
- Eliminación de un grupo de seguridad
- Asignar un grupo de seguridad a una instancia
- Cambiar el grupo de seguridad de una instancia

Crear un grupo de seguridad

Aunque puede utilizar el grupo de seguridad predeterminado para sus instancias, puede que desee crear sus propios grupos para reflejar las distintas funciones de desempeñan que juegan las instancias en su sistema.

De forma predeterminada, los grupos de seguridad nuevos comienzan con una única regla de salida que permite que todo el tráfico salga de las instancias. Debe añadir reglas para permitir el tráfico entrante o restringir el tráfico saliente.

El grupo de seguridad solo se puede utilizar en la VPC para la que se creó.

Console

Para crear un grupo de seguridad

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Grupos de seguridad.
3. Elija Create Security Group (Crear grupo de seguridad).
4. En la sección Detalles básicos haga lo siguiente.
   a. Introduzca un nombre descriptivo y una breve descripción para el grupo de seguridad. No se pueden editar después de crear el grupo de seguridad. El nombre y la descripción puede tener una longitud máxima de 255 caracteres. Los caracteres permitidos son a-z, A-Z, 0-9, espacios y ._-:/()#,@[]+=&;{}!$*.
   b. En VPC, elija la VPC.
5. Puede agregar reglas de grupo de seguridad ahora o más adelante. Para obtener más información, consulte Agregar reglas a un grupo de seguridad.
6. Puede agregar etiquetas ahora o más adelante. Para agregar una etiqueta, elija Agregar nueva etiqueta y, a continuación, ingrese la clave y el valor de la etiqueta.
7. Elija Crear grupo de seguridad.

Command line

Para crear un grupo de seguridad

Utilice uno de los siguientes comandos:

- create-security-group (AWS CLI)
- New-EC2SecurityGroup (AWS Tools for Windows PowerShell)

Copiar un grupo de seguridad

Puede crear un nuevo grupo de seguridad creando una copia de uno existente. Al copiar un grupo de seguridad, la copia se crea con las mismas reglas de entrada y salida que el grupo de seguridad original. Si el grupo de seguridad original está en una VPC, la copia se crea en la misma VPC a menos que especifique otra.

La copia recibe un nuevo ID de grupo de seguridad único y debe asignarle un nombre. También puede agregar una descripción.

No se puede copiar un grupo de seguridad de una región a otra.

Puede crear su grupo de seguridad mediante la consola de Amazon EC2.

Para copiar un grupo de seguridad

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Security Groups.
3. Seleccione el grupo de seguridad que desea copiar y elija Acciones, Copiar en nuevo grupo de seguridad.
4. Especifique un nombre y una descripción opcional, y cambie las reglas de VPC y grupo de seguridad si es necesario.
5. Seleccione Create (Crear).

Ver los grupos de seguridad

Puede ver información sobre los grupos de seguridad mediante uno de los métodos siguientes.

Console

Para ver los grupos de seguridad

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Security Groups.

3. Los grupos de seguridad aparecen en la lista. Para ver los detalles de un grupo de seguridad específico, incluidas sus reglas de entrada y salida, elija su ID en la columna ID de grupo de seguridad.

Command line

Para ver los grupos de seguridad

Utilice uno de los siguientes comandos.

- describe-security-groups (AWS CLI)
- describe-security-group-rules (AWS CLI)
- Get-EC2SecurityGroup (AWS Tools for Windows PowerShell)

Amazon EC2 Global View

Puede utilizar Amazon EC2 Global View a fin de ver los grupos de seguridad de todas las regiones para las que su cuenta de AWS se encuentra habilitada. Para obtener más información, consulte Amazon EC2 Global View.

Agregar reglas a un grupo de seguridad

Al agregar una regla a un grupo de seguridad, la nueva regla se aplica automáticamente a cualquier instancia que está asociada al grupo de seguridad. Es posible que haya un breve retraso antes de que se aplique la regla. Para obtener más información, consulte Reglas de grupo de seguridad para diferentes casos de uso y Reglas del grupo de seguridad.

Console

Para añadir una regla de entrada a un grupo de seguridad.

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Security Groups.
3. Seleccione el grupo de seguridad y elija Acciones, Editar reglas de entrada.
4. Para cada regla, elija Agregar regla y realice lo siguiente.
    a. En Tipo, elija el tipo de protocolo que desea permitir.

- En TCP personalizado o UDP personalizado, debe ingresar el intervalo de puertos que va a permitir. Por ejemplo, `0-99`.
- En ICMP personalizado, debe elegir el tipo de ICMP en Protocolo. El intervalo de puertos está configurado para usted. Por ejemplo, para permitir comandos ping, elija Echo Request desde Protocolo.
- Si elige cualquier otro tipo, el protocolo y el rango de puertos se configurarán en su nombre.

b. Para Fuente, realice una de las siguientes acciones para permitir el tráfico.

- Elija Personalizado y, a continuación, ingrese una dirección IP en notación CIDR, un bloque de CIDR, otro grupo de seguridad o una lista de prefijos.
- Elija Cualquier lugar para permitir que todo el tráfico del protocolo especificado llegue a su instancia. Esta opción agrega automáticamente el bloque IPv4 0.0.0.0/0 de CIDR como fuente. Si el grupo de seguridad está en una VPC habilitada para IPv6, esta opción agregará automáticamente una regla para el bloque de CIDR IPv6 ::/0.

> **Warning**
>
> Si elige Cualquier lugar, permite que todas las direcciones IPv4 e IPv6 tengan acceso a su instancia mediante el protocolo especificado. Si agrega reglas para los puertos 22 (SSH) o 3389 (RDP), debe autorizar solo a una dirección IP específica o a un rango de direcciones específico para acceder a su instancia.

- Elija Mi IP para permitir el tráfico entrante solo desde la dirección IPv4 pública de su equipo local.

c. En Descripción, especifique si lo desea una breve descripción de la regla.

5. Elija Vista previa de cambios, Guardar reglas.

Para agregar una regla de salida a un grupo de seguridad

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Security Groups.
3. Seleccione el grupo de seguridad y elija Acciones, Editar reglas de salida.
4. Para cada regla, elija Agregar regla y realice lo siguiente.

a. En Tipo, elija el tipo de protocolo que desea permitir.

- En TCP personalizado o UDP personalizado, debe ingresar el intervalo de puertos que va a permitir. Por ejemplo, `0-99`.
- En ICMP personalizado, debe elegir el tipo de ICMP en Protocolo. El intervalo de puertos está configurado para usted.
- Si elige cualquier otro tipo, el protocolo y el rango de puertos se configurarán de forma automática.

b. En Destino, siga uno de estos procedimientos.

- Elija Personalizado y, a continuación, escriba una dirección IP en notación CIDR, un bloque de CIDR, otro grupo de seguridad o una lista de prefijos para la que permitir el tráfico saliente.
- Elija En cualquier lugar para permitir el tráfico saliente en todas las direcciones IP. Esta opción agrega automáticamente el bloque de CIDR IPv4 0.0.0.0/0 como destino.

  Si el grupo de seguridad está en una VPC habilitada para IPv6, esta opción agregará automáticamente una regla para el bloque de CIDR IPv6 ::/0.
- Elija Mi IP para permitir el tráfico saliente solo a la dirección IPv4 pública del equipo local.

c. En Descripción, especifique una breve descripción de la regla.

5. Seleccione Vista previa de cambios, Confirmar.

Command line

Para agregar reglas a un grupo de seguridad

Utilice uno de los siguientes comandos.

- authorize-security-group-ingress (AWS CLI)
- Grant-EC2SecurityGroupIngress (AWS Tools for Windows PowerShell)

Para agregar una o más reglas de salida a un grupo de seguridad

Utilice uno de los siguientes comandos.

- authorize-security-group-egress (AWS CLI)

- Grant-EC2SecurityGroupEgress (AWS Tools for Windows PowerShell)

Actualizar reglas de los grupos de seguridad

Puede actualizar una regla de grupo de seguridad mediante uno de los métodos siguientes. La regla actualizada se aplica automáticamente a todas las instancias asociadas al grupo de seguridad.

Console

Al modificar el protocolo, el intervalo de puertos o el origen o destino de una regla de grupo de seguridad existente mediante la consola, esta elimina la regla existente y agrega una nueva automáticamente.

Para actualizar una regla de un grupo de seguridad

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Security Groups.
3. Seleccione el grupo de seguridad.
4. Elija Acciones y Editar reglas de entrada para actualizar una regla de tráfico de entrada, o bien Acciones y Editar reglas de salida para actualizar una regla de tráfico de salida.
5. Actualice la regla según sea necesario.
6. Seleccione Vista previa de cambios, Confirmar.

Para etiquetar una regla de grupo de seguridad

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Security Groups.
3. Seleccione el grupo de seguridad.
4. En la pestaña Reglas de entrada o Reglas de salida, seleccione la casilla de verificación correspondiente a la regla y, luego, elija Administrar etiquetas.
5. La página Administrar etiquetas muestra las etiquetas asignadas a la regla. Para agregar una etiqueta, elija Agregar etiqueta e ingrese la clave y el valor de la etiqueta. Para eliminar una etiqueta, elija Remove (Eliminar) junto a la etiqueta que desee eliminar.
6. Elija Guardar cambios.

Command line

No puede modificar el protocolo, el rango de puertos o el origen o destino de una regla existente mediante la API de Amazon EC2 o una herramienta de línea de comandos. En su lugar, debe eliminar la regla existente y añadir una nueva. Sin embargo, puede actualizar la descripción de una regla existente.

Para actualizar una regla

Utilice uno de los siguientes comandos.

- modify-security-group-rules (AWS CLI)

Para actualizar la descripción de una regla de entrada existente

Utilice uno de los siguientes comandos.

- update-security-group-rule-descriptions-ingress (AWS CLI)
- Update-EC2SecurityGroupRuleIngressDescription (AWS Tools for Windows PowerShell)

Para actualizar la descripción de una regla de salida existente

Utilice uno de los siguientes comandos.

- update-security-group-rule-descriptions-egress (AWS CLI)
- Update-EC2SecurityGroupRuleEgressDescription (AWS Tools for Windows PowerShell)

Para etiquetar una regla de grupo de seguridad

Utilice uno de los siguientes comandos.

- create-tags (AWS CLI)
- New-EC2Tag (AWS Tools for Windows PowerShell)

Eliminar reglas de un grupo de seguridad

Al eliminar una regla de un grupo de seguridad, el cambio se aplica automáticamente a cualquier instancia asociada al grupo de seguridad.

Puede eliminar reglas de un grupo de seguridad mediante uno de los métodos siguientes.

Console

Para eliminar una regla de grupo de seguridad

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Security Groups.
3. Seleccione el grupo de seguridad que desea actualizar, elija Acciones, y, a continuación, elija Editar reglas de entrada para eliminar una regla de entrada o Editar reglas de salida para eliminar una regla de salida.
4. Seleccione el botón Eliminar situado a la derecha de la regla que desea eliminar.
5. Seleccione Guardar reglas. También puede seleccionar Vista previa de los cambios, revisar los cambios y elegir Confirmar.

Command line

Para eliminar una o más reglas de entrada de un grupo de seguridad

Utilice uno de los siguientes comandos.

- revoke-security-group-ingress (AWS CLI)
- Revoke-EC2SecurityGroupIngress (AWS Tools for Windows PowerShell)

Para eliminar una o más reglas de salida de un grupo de seguridad

Utilice uno de los siguientes comandos.

- revoke-security-group-egress (AWS CLI)
- Revoke-EC2SecurityGroupEgress (AWS Tools for Windows PowerShell)

Eliminación de un grupo de seguridad

Un grupo de seguridad asociado a una instancia no se puede eliminar. El grupo de seguridad predeterminado no se puede eliminar. No se puede eliminar un grupo de seguridad al que hace referencia una regla en otro grupo de seguridad en la misma VPC. Si hace referencia al grupo de seguridad una de sus propias reglas, debe eliminar la regla antes de poder eliminar el grupo de seguridad.

Console

Para eliminar un grupo de seguridad

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Security Groups.
3. Seleccione un grupo de seguridad y elija Acciones, Eliminar grupo de seguridad.
4. Cuando se le pida confirmación, seleccione Eliminar.

Command line

Para eliminar un grupo de seguridad

Utilice uno de los siguientes comandos.

- delete-security-group (AWS CLI)
- Remove-EC2SecurityGroup (AWS Tools for Windows PowerShell)

Asignar un grupo de seguridad a una instancia

Puede asignar uno o más grupos de seguridad a una instancia cuando lance dicha instancia. También puede especificar uno o más grupos de seguridad en una plantilla de lanzamiento. Los grupos de seguridad se asignan a todas las instancias que se lancen mediante la plantilla de lanzamiento.

- Para asignar un grupo de seguridad a una instancia en el momento en que se lanza, consulte Network settings (Configuración de red) de iniciar una instancia mediante parámetros definidos (nueva consola) o Paso 6: Configurar un grupo de seguridad (consola antigua).
- Para especificar un grupo de seguridad en una plantilla de lanzamiento, consulte Network settings (Configuración de red) de Creación de una plantilla de inicialización a partir de parámetros.

Cambiar el grupo de seguridad de una instancia

Después de iniciar una instancia, puede cambiar sus grupos de seguridad mediante su agregado o eliminación.

Requisitos

- El estado de la instancia debe ser `running` o `stopped`.
- Un grupo de seguridad es específico de una VPC. Puede asignar un grupo de seguridad a una o más instancias lanzadas en la VPC para la que creó el grupo de seguridad.

Console

Para cambiar los grupos de seguridad de una instancia

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancias).
3. Seleccione la instancia y, a continuación, elija Acciones, Seguridad, Cambiar grupos de seguridad.
4. En Grupos de seguridad asociados, seleccione un grupo de seguridad de la lista y elija Agregar grupo de seguridad.

   Para quitar un grupo de seguridad ya asociado, elija Quitar para ese grupo de seguridad.
5. Seleccione Guardar.

Command line

Para cambiar los grupos de seguridad de una instancia

Utilice uno de los siguientes comandos.

- modify-instance-attribute (AWS CLI)
- Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

Reglas de grupo de seguridad para diferentes casos de uso

Puede crear un grupo de seguridad y agregar reglas que reflejen el rol de la instancia que está asociada al grupo de seguridad. Por ejemplo, una instancia configurada como servidor web necesita reglas de grupo de seguridad que permitan el acceso HTTP y HTTPS entrante. Del mismo modo, una instancia de la base de datos necesita reglas que permitan el acceso para el tipo de base de datos, como el acceso a través del puerto 3306 para MySQL.

A continuación, se muestran ejemplos de los tipos de reglas que puede agregar a grupos de seguridad para tipos concretos de acceso.

Ejemplos

- Reglas del servidor web
- Reglas del servidor de bases de datos
- Reglas para conectarse a las instancias desde un equipo
- Reglas para conectarse a las instancias desde una instancia con el mismo grupo de seguridad
- Reglas para hacer ping/ICMP
- Reglas del servidor DNS
- Reglas de Amazon EFS
- Reglas de Elastic Load Balancing
- Reglas de interconexión de VPC

Reglas del servidor web

Las siguientes reglas de entrada permiten el acceso HTTP y HTTPS de cualquier dirección IP. Si la VPC está habilitada para IPv6, puede agregar reglas para controlar el tráfico HTTP y HTTPS de entrada de direcciones IPv6.

Tipo de protocolo	Número de protocolo	Puerto	IP de origen	Notas
TCP	6	80 (HTTP)	0.0.0.0/0	Permite el acceso de HTTP entrante de cualquier dirección IPv4.
TCP	6	443 (HTTPS)	0.0.0.0/0	Permite el acceso HTTPS entrante de cualquier dirección IPv4.
TCP	6	80 (HTTP)	::/0	Permite el acceso HTTP entrante desde cualquier dirección IPv6

Tipo de protocolo	Número de protocolo	Puerto	IP de origen	Notas
TCP	6	443 (HTTPS)	::/0	Permite el acceso HTTPS entrante desde cualquier dirección IPv6

Reglas del servidor de bases de datos

Las siguientes reglas de entrada son ejemplos de reglas que podría agregar para el acceso a bases de datos, según el tipo de base de datos que esté ejecutando en la instancia. Para obtener más información acerca de las instancias de Amazon RDS, consulte la Guía del usuario de Amazon RDS.

Para la IP de origen, especifique uno de los siguientes:

- Una dirección IP específica o un rango de direcciones IP (con la notación de bloques de CIDR) de la red local
- Un ID de grupo de seguridad para un grupo de instancias que obtengan acceso a la base de datos

Tipo de protocolo	Número de protocolo	Puerto	Notas
TCP	6	1433 (MS SQL)	El puerto predeterminado para obtener acceso a una base de datos Microsoft SQL Server, por ejemplo, en una instancia Amazon RDS.
TCP	6	3306 (MYSQL/Aurora)	El puerto predeterminado para obtener acceso a una base de datos MySQL o Aurora, por ejemplo, en una instancia Amazon RDS.
TCP	6	5439 (Redshift)	El puerto predeterminado para obtener acceso a una base de datos de clúster Amazon Redshift.

Tipo de protocolo	Número de protocolo	Puerto	Notas
TCP	6	5432 (PostgreSQL)	El puerto predeterminado para obtener acceso a una base de datos PostgreSQL, por ejemplo, en una instancia Amazon RDS.
TCP	6	1521 (Oracle)	El puerto predeterminado para obtener acceso a una base de datos Oracle, por ejemplo, en una instancia Amazon RDS.

Opcionalmente, puede restringir el tráfico saliente desde los servidores de base de datos. Por ejemplo, es posible que desee permitir el acceso a Internet para actualizaciones de software y restringir todos los demás tipos de tráfico. Primero debe eliminar la regla de salida predeterminada que permite todo el tráfico de salida.

Tipo de protocolo	Número de protocolo	Puerto	IP de destino	Notas
TCP	6	80 (HTTP)	0.0.0.0/0	Permite el acceso HTTP saliente a cualquier dirección IPv4.
TCP	6	443 (HTTPS)	0.0.0.0/0	Permite el acceso HTTPS saliente a cualquier dirección IPv4.
TCP	6	80 (HTTP)	::/0	(Solo para VPC habilitada para IPv6) Permite el acceso HTTP saliente a cualquier dirección IPv6.
TCP	6	443 (HTTPS)	::/0	(Solo para VPC habilitada para IPv6) Permite el acceso

Tipo de protocolo	Número de protocolo	Puerto	IP de destino	Notas
				HTTPS saliente a cualquier dirección IPv6.

Reglas para conectarse a las instancias desde un equipo

Para conectarse a una instancia, el grupo de seguridad debe tener reglas de entrada que permitan el acceso SSH (para instancias de Linux) o el acceso RDP (para instancias de Windows).

Tipo de protocolo	Número de protocolo	Puerto	IP de origen
TCP	6	22 (SSH)	La dirección IPv4 pública de su equipo o un rango de las direccion es IP en su red local. Si la VPC está habilitada para IPv6 y la instancia tiene una dirección IPv6, puede escribir una dirección IPv6 o un rango.
TCP	6	3389 (RDP)	La dirección IPv4 pública de su equipo o un rango de las direccion es IP en su red local. Si la VPC está habilitada para IPv6 y la instancia tiene una dirección IPv6, puede escribir una dirección IPv6 o un rango.

Reglas para conectarse a las instancias desde una instancia con el mismo grupo de seguridad

Para permitir que las instancias asociadas al mismo grupo de seguridad se comuniquen unas con otras, debe agregar explícitamente reglas para ello.

> **Note**
>
> Si configura rutas para reenviar el tráfico entre dos instancias en subredes diferentes a través de un dispositivo de middlebox, debe asegurarse de que los grupos de seguridad de ambas instancias permiten que el tráfico fluya entre las instancias. El grupo de seguridad de cada instancia debe hacer referencia a la dirección IP privada de la otra instancia, o al rango CIDR de la subred que contiene la otra instancia, como fuente. Si hace referencia al grupo de seguridad de la otra instancia como fuente, esto no permite que el tráfico fluya entre las instancias.

La siguiente tabla describe la regla de entrada para un grupo de seguridad que permite que las instancias asociadas se comuniquen entre sí. La regla permite todo tipo de tráfico.

Tipo de protocolo	Número de protocolo	Puertos	IP de origen
-1 (Todos)	-1 (Todos)	-1 (Todos)	El ID del grupo de seguridad, o bien el rango CIDR de la subred que contiene la otra instancia (consulte la nota).

Reglas para hacer ping/ICMP

El comando ping es un tipo de tráfico de ICMP. Para hacer un ping a la instancia, debe agregar una de las siguientes reglas de entrada de ICMP.

Tipo	Protocolo	Origen		
ICMP personalizado: IPv4	Repetir solicitud	La dirección IPv4 pública del equipo, una dirección IPv4 específica o una dirección		

Tipo	Protocolo	Origen		
		IPv4 o IPv6 de cualquier lugar.		
Todos ICMP: IPv4	ICMP de IPv4 (1)	La dirección IPv4 pública del equipo, una dirección IPv4 específica o una dirección IPv4 o IPv6 de cualquier lugar.		

Para utilizar el comando ping6 para hacer ping a la dirección IPv6 de su instancia, debe agregar la siguiente regla de entrada de ICMPv6.

Tipo	Protocolo	Origen		
Todos los ICMP: IPv6	ICMP de IPv6 (58)	La dirección IPv6 del equipo, una dirección IPv4 específica o una dirección IPv4 o IPv6 desde cualquier lugar.		

Reglas del servidor DNS

Si ha configurado su instancia de EC2 como un servidor DNS, debe asegurarse de que el tráfico TCP y UDP pueden llegar al servidor DNS a través del puerto 53.

Para la IP de origen, especifique uno de los siguientes:

- Una dirección IP o un rango de direcciones IP (con la notación de bloques de CIDR) de una local
- El ID de un grupo de seguridad para el conjunto de instancias de la red que requieran acceso al servidor DNS

Tipo de protocolo	Número de protocolo	Puerto
TCP	6	53
UDP	17	53

Reglas de Amazon EFS

Si está utilizando un sistema de archivos de Amazon EFS con las instancias Amazon EC2, el grupo de seguridad que asocia a los destinos de montaje de Amazon EFS debe permitir el tráfico a través del protocolo NFS.

Tipo de protocolo	Número de protocolo	Puertos	IP de origen	Notas
TCP	6	2049 (NFS)	El ID del grupo de seguridad	Permite el acceso NFS de entrada desde los recursos (incluido el destino de montaje) asociados a este grupo de seguridad.

Para montar un sistema de archivos de Amazon EFS en la instancia Amazon EC2, debe conectarse a la instancia. Por consiguiente, el grupo de seguridad asociado a su instancia debe tener reglas que permitan el tráfico SSH entrante de su equipo local o red local.

Tipo de protocolo	Número de protocolo	Puertos	IP de origen	Notas
TCP	6	22 (SSH)	El rango de direccion es IP del equipo local o el rango de direcciones IP (con la notación de bloques de CIDR) de la red.	Permite el acceso SSH entrante desde el equipo local.

Reglas de Elastic Load Balancing

Si está utilizando un balanceador de carga, el grupo de seguridad asociado al balanceador debe tener reglas que permitan la comunicación con sus instancias o destinos. Para obtener más información, consulte Configurar grupos de seguridad para Classic Load Balancer en la Guía del usuario de Classic Load Balancers y Grupos de seguridad para el Application Load Balancer en la Guía del usuario de Application Load Balancers.

Reglas de interconexión de VPC

Puede actualizar las reglas entrantes o salientes de los grupos de seguridad de su VPC para que hagan referencia a grupos de seguridad de la VPC del mismo nivel. De este modo, garantizará el tráfico entrante y saliente de las instancias asociadas al grupo de seguridad al que se hace referencia en la VPC del mismo nivel. Para obtener más información sobre cómo configurar los grupos de seguridad para interconexión de VPC, consulte Actualización de los grupos de seguridad para que hagan referencia a grupos de la VPC del mismo nivel.

NitroTPM

NitroTPM, el módulo de confianza de la plataforma Nitro, es un dispositivo virtual que proporciona el AWS Nitro System y se ajusta a la especificación de TPM 2.0. Almacena de forma segura los artefactos (como contraseñas, certificados o claves de cifrado) que se utilizan para autenticar la instancia. NitroTPM puede generar claves y utilizarlas para funciones criptográficas (como hash, firma, cifrado y descifrado).

NitroTPM proporciona arranque medido, un proceso en el que el cargador de arranque y el sistema operativo crean hash criptográficos de cada binario de arranque y los combinan con los valores anteriores de los registros de configuración de plataformas (PCR) internos de NitroTPM. Con el arranque medido, puede obtener valores de PCR firmados de NitroTPM y utilizarlos para demostrar a las entidades remotas la integridad del software de arranque de la instancia. Esto se denomina declaración remota.

Con NitroTPM, las claves y los secretos se pueden etiquetar con un valor PCR específico para que nunca se pueda acceder a ellos si cambia el valor de la PCR y, con ello, la integridad de la instancia. Esta forma especial de acceso condicional se denomina sellado y revelado. Tecnologías de sistemas operativos, como BitLocker, pueden utilizar NitroTPM para sellar una clave de descifrado de unidad de modo que esta solo se pueda descifrar cuando el sistema operativo arrancó correctamente y se encuentra en un buen estado conocido.

Para utilizar NitroTPM, debe seleccionar una imagen de máquina de Amazon (AMI) que se ha configurado para la compatibilidad con NitroTPM y, a continuación, utilizar la AMI para inicializar instancias basadas en el AWS Nitro System. Puede seleccionar una de las AMI de Amazon creadas previamente o crear una.

Costos

No se aplica ningún costo adicional por el uso de NitroTPM. Solo pagará por los recursos subyacentes que utilice.

Temas

Consideraciones

Las siguientes consideraciones se aplican cuando se utiliza NitroTPM:

- Los volúmenes BitLocker cifrados con claves basadas en NitroTPM solo se pueden utilizar en la instancia original.
- El estado de NitroTPM no se incluye en las instantáneas de Amazon EBS.
- El estado de NitroTPM no se incluye en imágenes VM Import/Export.
- La compatibilidad con NitroTPM se habilita al especificar un valor de `v2.0` para el parámetro `tpm-support` al crear una AMI. Después de iniciar una instancia con la AMI, no podrá modificar los atributos de dicha instancia. Las instancias con NitroTPM no admiten la API ModifyInstanceAttribute.
- Solo puede crear una AMI con NitroTPM configurado mediante la API RegisterImage al usar la AWS CLI y no con la consola de Amazon EC2.
- NitroTPM no es compatible con Outposts.
- NitroTPM no es compatible en zonas locales o zonas Wavelength.

Requisitos previos para habilitar en la inicialización

Para iniciar una instancia con NitroTPM habilitado, se debe cumplir con los siguientes requisitos previos.

instancias de Linux

AMI

Requiere una AMI con NitroTPM habilitado.

En la actualidad, no hay AMI de Amazon Linux con NitroTPM habilitado. Para utilizar una AMI admitida, debe realizar varios pasos de configuración en su propia AMI de Linux. Para obtener más información, consulte Creación de una AMI de Linux para la compatibilidad con NitroTPM.

Sistema operativo

La AMI debe incluir un sistema operativo con un controlador de búfer de respuesta del comando (CRB) TPM 2.0. La mayoría de los sistemas operativos actuales, tales como Amazon Linux 2, cuentan con un controlador CRB TPM 2.0.

Modo de arranque UEFI

NitroTPM requiere que una instancia se ejecute en modo de arranque UEFI, lo que requiere que la AMI esté configurada para este modo de arranque. Para obtener más información, consulte Arranque seguro UEFI.

instancias de Windows

AMI

Requiere una AMI con NitroTPM habilitado.

Las siguientes AMI de Windows están preconfiguradas para habilitar NitroTPM y el modo Arranque seguro UEFI con claves de Microsoft:

- TPM-Windows_Server-2022-English-Core-Base
- TPM-Windows_Server-2022-English-Full-Base
- TPM-Windows_Server-2022-English-Full-SQL_2022_Enterprise
- TPM-Windows_Server-2022-English-Full-SQL_2022_Standard

- TPM-Windows_Server-2019-English-Core-Base
- TPM-Windows_Server-2019-English-Full-Base
- TPM-Windows_Server-2019-English-Full-SQL_2019_Enterprise
- TPM-Windows_Server-2019-English-Full-SQL_2019_Standard
- TPM-Windows_Server-2016-English-Core-Base
- TPM-Windows_Server-2016-English-Full-Base

Actualmente, no se admite la importación de Windows con NitroTPM mediante el comando import-image.

Sistema operativo

La AMI debe incluir un sistema operativo con un controlador de búfer de respuesta del comando (CRB) TPM 2.0. La mayoría de los sistemas operativos actuales, tales como TPM-Windows_Server-2022-English-Full-Base, cuentan con un controlador CRB TPM 2.0.

Modo de arranque UEFI

NitroTPM requiere que una instancia se ejecute en modo de arranque UEFI, lo que requiere que la AMI esté configurada para este modo de arranque. Para obtener más información, consulte Arranque seguro UEFI.

Tipos de instancias

Debe utilizar uno de los siguientes tipos de instancia virtualizada:

- De uso general: M5, M5a, M5ad, M5d, M5dn, M5n, M5zn, M6a, M6i, M6id, M6idn, M6in, M7a, M7i, M7i-flex, T3, T3a
- Optimizadas para la computación: C5, C5a, C5ad, C5d, C5n, C6a, C6i, C6id, C6in, C7a, C7i, C7i-flex
- Optimizadas para la memoria: R5, R5a, R5ad, R5b, R5d, R5dn, R5n, R6a, R6i, R6idn, R6in, R6id, R7a, R7i, R7iz, U7i-12tb, U7in-16tb, U7in-24tb, U7in-32tb, X2idn, X2iedn, X2iezn, z1d
- Optimizadas para el almacenamiento: D3, D3en, I3en, I4i
- De computación acelerada: G4dn, G5, G6, Gr6, Inf1, Inf2
- De computación de alto rendimiento: Hpc6a, Hpc6id

> **Note**
>
> No se admiten las instancias basadas en Graviton, las instancias Xen, las instancias de Mac y las instancias bare metal.

Creación de una AMI de Linux para la compatibilidad con NitroTPM

Configure una AMI de Linux para la compatibilidad con NitroTPM cuando registre la AMI. No puede configurar la compatibilidad con NitroTPM más adelante.

Para obtener la lista de AMI de Windows que están preconfiguradas para la compatibilidad con NitroTPM, consulte Requisitos previos para habilitar en la inicialización.

Para registrar una AMI de Linux para la compatibilidad con NitroTPM

1. Lance una instancia temporal con la AMI de Linux obligatoria.
2. Cuando la instancia alcance el estado `running`, cree una instantánea del volumen raíz de la instancia.
3. Registre la nueva AMI. Utilice el comando register-image. En `--tpm-support`, especifique `v2.0`. En `--boot-mode`, especifique `uefi`. Y especifique una asignación de dispositivos de bloques para el volumen raíz mediante la instantánea que creó en el paso anterior.

   ```
   aws ec2 register-image \
       --name my-image \
       --boot-mode uefi \
       --architecture x86_64 \
       --root-device-name /dev/xvda \
       --block-device-mappings DeviceName=/dev/xvda,Ebs={SnapshotId=snapshot_id} \
       --tpm-support v2.0
   ```

   Resultado previsto

   ```
   {
   "ImageId": "ami-0123456789example"
   }
   ```

4. Terminar la instancia temporal que se lanzó en el paso 1 si esta ya no es necesaria.

Verificación de si una AMI está habilitada para NitroTPM

Puede utilizar `describe-images` o `describe-image-attributes` para verificar si una AMI está habilitada para NitroTPM.

Verificación de si una AMI está habilitada para NitroTPM mediante **`describe-images`**

Utilice el comando describe-images y especifique el ID de la AMI.

```
aws ec2 describe-images --image-ids ami-0123456789example
```

Si NitroTPM está habilitado para la AMI, `"TpmSupport": "v2.0"` aparece en el resultado.

```
{
    "Images": [
        {
        ...
        "BootMode": "uefi",
        ...
        "TpmSupport": "v2.0"
        }
    ]
}
```

Verificación de si una AMI está habilitada para NitroTPM mediante **`describe-image-attribute`**

Utilice el comando describe-image-attribute y especifique el parámetro `attribute` con el valor `tpmSupport`.

> **Note**
>
> Debe ser el propietario de la AMI para llamar a `describe-image-attribute`.

```
aws ec2 describe-image-attribute \
    --region us-east-1 \
    --image-id ami-0123456789example \
    --attribute tpmSupport
```

Si NitroTPM está habilitado para la AMI, el valor de `TpmSupport` es `"v2.0"`. Tenga en cuenta que `describe-image-attribute` solo arroja los atributos especificados en la solicitud.

```
{
    "ImageId": "ami-0123456789example",
    "TpmSupport": {
        "Value": "v2.0"
    }
}
```

Habilitar o dejar de utilizar NitroTPM en una instancia

Al iniciar una instancia desde una AMI que tiene habilitada la compatibilidad con NitroTPM, la instancia se inicia con NitroTPM habilitado. Puede configurar la instancia para que deje de utilizar NitroTPM. Puede verificar si una instancia está habilitada para NitroTPM.

Temas

Lanzamiento de una instancia con NitroTPM habilitado

Cuando lance una instancia con los requisitos previos, NitroTPM se habilita automáticamente en dicha instancia. Solo puede habilitar NitroTPM en una instancia durante el lanzamiento. Para obtener más información acerca de cómo iniciar una instancia, consulte iniciar la instancia.

Dejar de utilizar NitroTPM en una instancia

Después de iniciar una instancia con NitroTPM habilitado, no puede desactivar NitroTPM para dicha instancia. Sin embargo, puede configurar el sistema operativo para que deje de utilizar NitroTPM al desactivar el controlador de dispositivo TPM 2.0 en la instancia mediante las siguientes herramientas:

- [Instancias de Linux] Utilice tpm-tools.
- [Instancias de Windows] Utilice la consola de administración de TPM, tpm.msc.

Para obtener más información sobre la desactivación del controlador de dispositivo, consulte la documentación de su sistema operativo.

Verificación de si se puede acceder a NitroTPM dentro de la instancia

Verificación de si una instancia está habilitada para la compatibilidad con NitroTPM mediante la AWS CLI

Use el comando describe-instances de AWS CLI y especifique el ID de la instancia. Actualmente, la consola de Amazon EC2 no muestra el campo `TpmSupport`.

```
aws ec2 describe-instances --instance-ids i-0123456789example
```

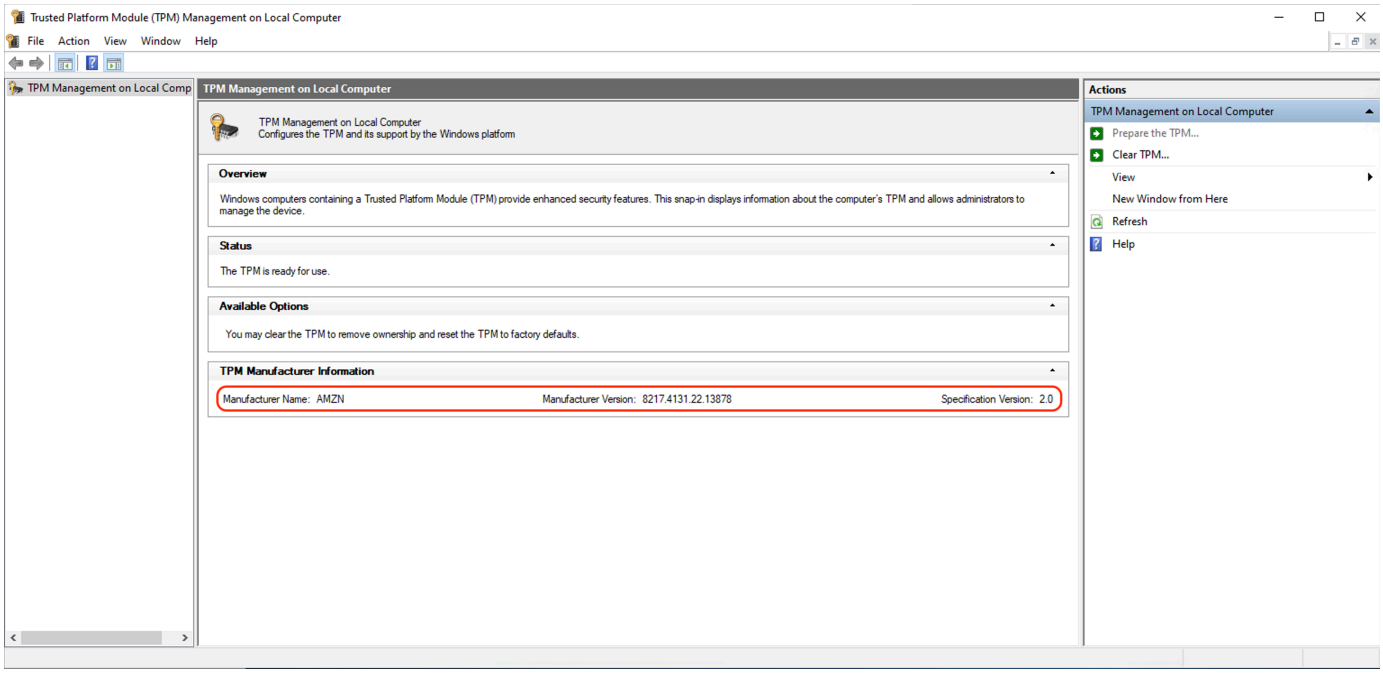
Si la compatibilidad con NitroTPM está habilitada en la instancia, `"TpmSupport": "v2.0"` aparece en el resultado.

```
"Instances": {
              "InstanceId":"0123456789example",
              "InstanceType":"c5.large",
              ...
              "BootMode": "uefi",
              "TpmSupport": "v2.0"
              ...
              }
```

(Instancias de Windows) Para verificar la accesibilidad de NitroTPM dentro de una instancia de Windows de Amazon EC2

1. Conéctese a la instancia sw EC2 de Windows.
2. En la instancia, ejecute el programa tpm.msc.

   Aparecerá la ventana Administración de TPM en computadora local.
3. Compruebe el campo Información del fabricante de TPM. Contiene el nombre del fabricante y la versión de NitroTPM en la instancia.



Recupere la clave de aprobación pública de una instancia

Puede recuperar de forma segura la clave de aprobación pública de una instancia en cualquier momento con la AWS CLI.

Para recuperar la clave de aprobación pública de una instancia

Use el comando get-instance-tpm-ek-pub de la AWS CLI.

Ejemplo 1

El siguiente comando de ejemplo obtiene la clave de aprobación pública `rsa-2048` en formato `tpmt` para la instancia `i-01234567890abcdef`.

```
$ aws ec2 get-instance-tpm-ek-pub \
--instance-id i-01234567890abcdef \
--key-format tpmt \
--key-type rsa-2048
```

A continuación, se muestra un ejemplo del resultado.

```
{
    "InstanceId": "i-01234567890abcdef",
```

```
    "KeyFormat": "tpmt",
    "KeyType": "rsa-2048",
    "KeyValue": "AAEACwADALIAIINxl2dEhLEXAMPLEUal1yT9UtduBlILZPKh2hszFGmqAAYAgABDA
    EXAMPLEAAABAOiRd7WmgtdGNoV1h/AxmW+CXExblG8pEUfNm0LOLiYnEXAMPLERqApiFa/UhvEYqN4
    Z7jKMD/usbhsQaAB1gKA5RmzuhSazHQkax7EXAMPLEzDthlS7HNGuYn5eG7qnJndRcakS+iNxT8Hvf
    0S1ZtNuItMs+Yp4SO6aU28MT/JZkOKsXIdMerY3GdWbNQz9AvYbMEXAMPLEPyHfzgVO0QTTJVGdDxh
    vxtXCOu9GYf0crbjEXAMPLEd4YTbWdDdgOKWF9fjzDytJSDhrLAOUctNzHPCd/92l5zEXAMPLEOIFA
    Ss50C0/802c17W2pMSVHvCCa9lYCiAfxH/vYKovAAE="
}
```

Ejemplo 2

El siguiente comando de ejemplo obtiene la clave de aprobación pública `rsa-2048` en formato `der` para la instancia `i-01234567890abcdef`.

```
$ aws ec2 get-instance-tpm-ek-pub \
--instance-id i-01234567890abcdef \
--key-format der \
--key-type rsa-2048
```

A continuación, se muestra un ejemplo del resultado.

```
{
    "InstanceId": "i-01234567890abcdef",
    "KeyFormat": "der",
    "KeyType": "rsa-2048",
    "KeyValue": "MIIBIjANBgEXAMPLEw0BAQEFAAOCAQ8AMIIBCgKCAQEA6JF3taEXAMPLEXWH8DGZb4
    JcTFuUbykRR82bQs4uJifaKSOv5NGoEXAMPLEG8Rio3hnuMowP+6xuGxBoAHWAoDlGbO6FJrMdEXAMP
    LEnYUHvMO2GVLsc0a5ifl4buqcmd1FxqRL6I3FPwe9/REXAMPLE0yz5inhI7ppTbwxP8lmQ4qxch0x6
    tjcZ1Zs1DP0EXAMPLERUYLQ/Id/OBU7RBNMlUZ0PGG/G1cI670Zh/RytuOdx9iEXAMPLEtZ0N2A4pYX
    1+PMPK0lIOGssA5Ry03Mc8J3/3aXnOD2/ASRQ4gUBKznQLT/zTZEXAMPLEJUe8IJr2VgKIB/Ef+9gqi
    8AAQIDAQAB"
}
```

Credential Guard para instancias de Windows

El sistema AWS Nitro es compatible con Credential Guard para instancias de Windows de Amazon Elastic Compute Cloud (Amazon EC2). Credential Guard es una característica de seguridad basada en la virtualización (VBS) de Windows que permite crear entornos aislados para proteger los activos de seguridad, como las credenciales de usuario de Windows y el cumplimiento de la integridad

del código, más allá de las protecciones del kernel de Windows. Al ejecutar instancias de EC2 de Windows, Credential Guard utiliza el sistema AWS Nitro para evitar que las credenciales de inicio de sesión de Windows se extraigan de la memoria del sistema operativo.

Contenido

Requisitos previos

Su instancia de Windows debe cumplir los siguientes requisitos previos para utilizar Credential Guard:

Imágenes de máquina de Amazon (AMI)

La AMI debe estar preconfigurada para habilitar NitroTPM y el UEFI Secure Boot. Para obtener más información acerca de las AMI, consulte the section called “Requisitos previos”.

Integridad de memoria

No se admite la integridad de memoria, también conocida como integridad del código del hipervisor (HVCI) o integridad de código aplicado por hipervisor. Antes de activar Credential Guard, debe asegurarse de que esta característica esté deshabilitada. Para obtener más información, consulte Cómo desactivar la integridad de memoria.

Tipos de instancias

Los siguientes tipos de instancias admiten Credential Guard en todos los tamaños: `C5`, `C5d`, `C5n`, `C6i`, `C6id`, `C6in`, `M5`, `M5d`, `M5dn`, `M5n`, `M5zn`, `M6i`, `M6id`, `M6idn`, `M6in`, `R5`, `R5b`, `R5d`, `R5dn`, `R5n`, `R6i`, `R6id`, `R6idn`, `R6in`.

> **Note**
>
> Si bien NitroTPM tiene algunos tipos de instancia obligatorios en común, el tipo de instancia debe ser uno de los anteriores para que sea compatible con Credential Guard.

Lanzamiento de una instancia compatible

Puede utilizar la consola de Amazon EC2 o AWS Command Line Interface (AWS CLI) para iniciar una instancia que sea compatible con Credential Guard. Necesitará un ID de AMI compatible para iniciar la instancia, que sea único para cada Región de AWS.

> **Tip**
>
> Puede utilizar el siguiente enlace para descubrir y iniciar instancias con AMI compatibles proporcionadas por Amazon en la consola de Amazon EC2: https://console.aws.amazon.com/ec2/v2/home?#Images:visibility=public-images;v=3;search=:TPM-Windows_Server;ownerAlias=amazon

Amazon EC2 console

Para iniciar una instancia mediante la consola de Amazon EC2

Siga estos pasos para lanzar una instancia y especificar un tipo de instancia compatible y una AMI de Windows preconfigurada.

AWS CLI

Para lanzar una instancia mediante la AWS CLI

Utilice el comando run-instances para lanzar una instancia con un tipo de instancia compatible y una AMI de Windows preconfigurada.

```
aws ec2 run-instances \
    --image-id resolve:ssm:/aws/service/ami-windows-latest/TPM-Windows_Server-2022-English-Full-Base \
    --instance-type c6i.large \
    --region us-east-1 \
    --subnet-id subnet-id
    --key-name key-name
```

PowerShell

Para lanzar una instancia mediante la AWS Tools for PowerShell

Utilice el comando New-EC2Instance para lanzar una instancia con un tipo de instancia compatible y una AMI de Windows preconfigurada.

```
New-EC2Instance `
    -ImageId resolve:ssm:/aws/service/ami-windows-latest/TPM-Windows_Server-2022-English-Full-Base `
    -InstanceType c6i.large `
    -Region us-east-1 `
    -SubnetId subnet-id `
    -KeyName key-name
```

Cómo desactivar la integridad de memoria

Puede utilizar el Editor de políticas de grupo local para desactivar la integridad de memoria en los escenarios compatibles. Se puede aplicar la siguiente instrucción para cada parámetro de configuración de la Protección basada en la virtualización de la integridad del código:

- Habilitada sin bloqueo: modifique la configuración a Desactivada para desactivar la integridad de memoria.
- Habilitada con bloqueo UEFI: la integridad de memoria se ha habilitado con el bloqueo UEFI. La integridad de memoria no se puede desactivar una vez que se haya habilitado con el bloqueo UEFI. Recomendamos crear una nueva instancia con la integridad de memoria desactivada y terminar la instancia no compatible si no está en uso.

Para desactivar la integridad de memoria con el Editor de políticas de grupos locales

1. Conéctese a su instancia como una cuenta de usuario con privilegios de administrador mediante el protocolo de escritorio remoto (RDP). Para obtener más información, consulte the section called “Conexión a la instancia de Windows mediante un cliente RDP”.
2. Abra el menú Inicio y busque **`cmd`** para abrir un símbolo del sistema.
3. Ejecute el siguiente comando para abrir el editor de políticas de grupo local: `gpedit.msc`
4. En el editor de políticas de grupo local, elija Configuración del equipo, Plantillas administrativas, Sistema, Device Guard.
5. Seleccione Activar seguridad basada en la virtualización y, a continuación, seleccione Editar configuración de políticas.
6. Abra el menú desplegable de configuración para Protección basada en la virtualización de la integridad de código, elija Desactivada y, a continuación, seleccione Aplicar.
7. Reinicie la instancia para aplicar los cambios.

Cómo activar Credential Guard

Después de iniciar una instancia de Windows con un tipo de instancia y una AMI compatibles, y tras confirmar que se ha desactivado la integridad de memoria, puede activar Credential Guard.

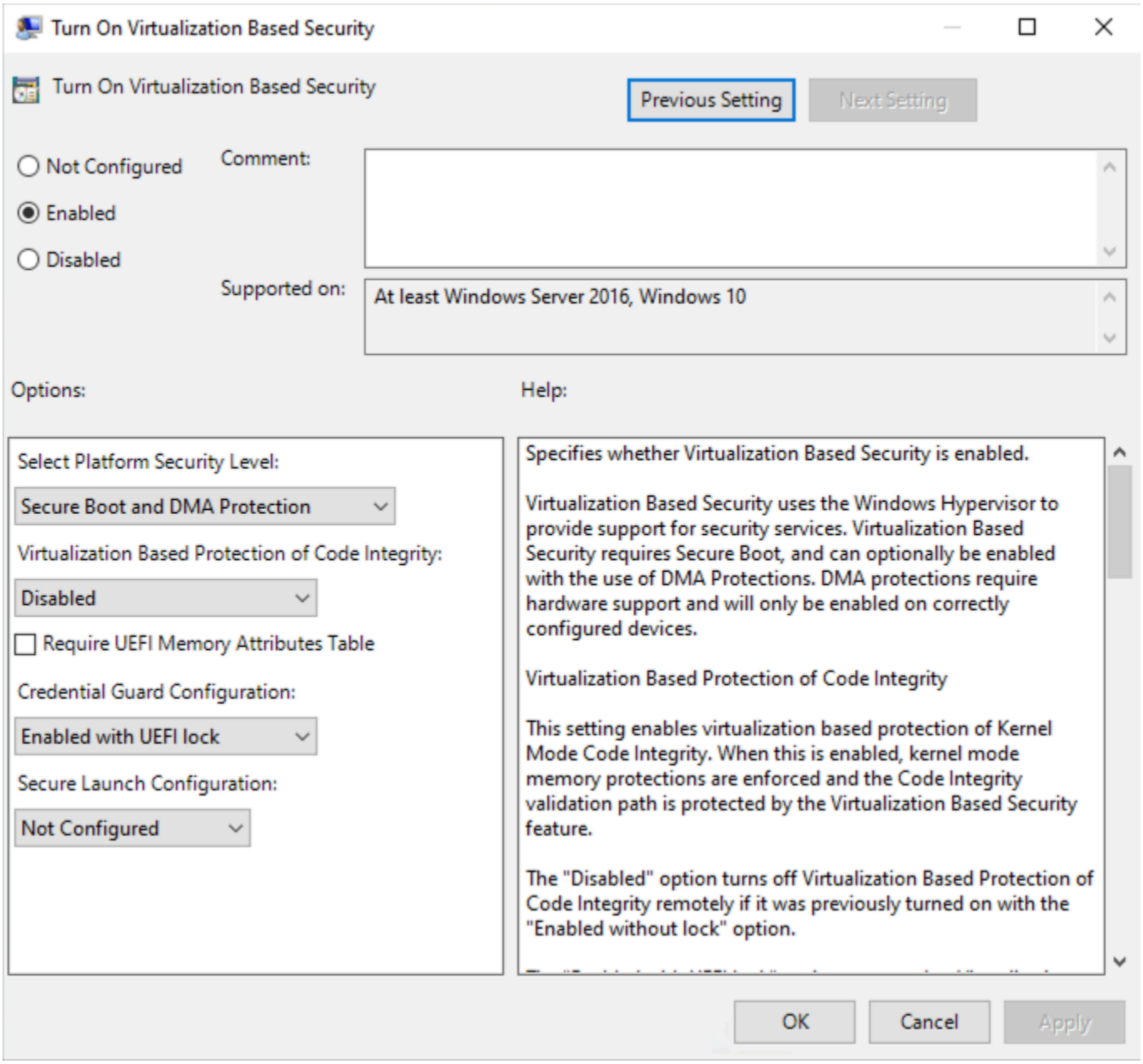
> **Important**
>
> Se requieren privilegios de administrador para realizar los siguientes pasos para activar Credential Guard.

Para activar Credential Guard

1. Conéctese a su instancia como una cuenta de usuario con privilegios de administrador mediante el protocolo de escritorio remoto (RDP). Para obtener más información, consulte the section called “Conexión a la instancia de Windows mediante un cliente RDP”.
2. Abra el menú Inicio y busque **`cmd`** para abrir un símbolo del sistema.
3. Ejecute el siguiente comando para abrir el editor de políticas de grupo local: `gpedit.msc`
4. En el editor de políticas de grupo local, elija Configuración del equipo, Plantillas administrativas, Sistema, Device Guard.
5. Seleccione Activar seguridad basada en la virtualización y, a continuación, seleccione Editar configuración de políticas.
6. Elija Habilitado en el menú Activar seguridad basada en la virtualización.
7. En Seleccionar nivel de seguridad de la plataforma, elija Arranque seguro y protección DMA.
8. En Configuración de Credential Guard, elija Habilitada con bloqueo de UEFI.

   > **Note**
   >
   > Las configuraciones de política restantes no son necesarias para habilitar Credential Guard y se pueden dejar como No configuradas.

   La siguiente imagen muestra los ajustes de VBS configurados como se ha descrito anteriormente:



9. Reinicie la instancia para aplicar la configuración.

Cómo comprobar que Credential Guard se esté ejecutando

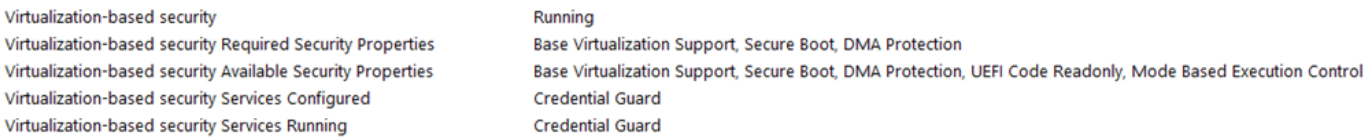
Puede utilizar la herramienta Información del sistema de Microsoft (`Msinfo32.exe`) para confirmar que Credential Guard se esté ejecutando.

> **Important**
>
> Primero debe reiniciar la instancia para terminar de aplicar la configuración de políticas necesaria para habilitar Credential Guard.

Para comprobar que Credential Guard se esté ejecutando

1. Conéctese a la instancia mediante el protocolo de escritorio remoto (RDP). Para obtener más información, consulte the section called “Conexión a la instancia de Windows mediante un cliente RDP”.
2. Dentro de la sesión RDP de su instancia, abra el menú Inicio y busque **`cmd`** para abrir un símbolo del sistema.
3. Para abrir Información del sistema ejecute el siguiente comando: `msinfo32.exe`
4. La herramienta Información del sistema de Microsoft muestra los detalles de la configuración de VBS. Junto a Servicios de seguridad basados en la virtualización, confirme que Credential Guard aparezca como En ejecución.

   La siguiente imagen muestra que VBS se está ejecutando, como se ha descrito anteriormente:



Opciones de almacenamiento para sus instancias de Amazon EC2

Amazon EC2 le ofrece opciones de almacenamiento de datos flexibles, rentables y de fácil uso para sus instancias. Cada opción presenta una combinación exclusiva de rendimiento y durabilidad. Las opciones de almacenamiento se pueden utilizar de forma independiente o combinadas para ajustarse a sus requisitos.

Amazon EBS

Amazon EBS ofrece volúmenes de almacenamiento por bloques duraderos que se pueden asociar a una instancia en ejecución y desasociar de ella. También puede asociar varios volúmenes de EBS a una instancia. Un volumen de EBS persiste independientemente de la duración de la instancia asociada. Puede cifrar sus volúmenes de EBS. Para mantener una copia de seguridad de los datos, puede crear instantáneas de los volúmenes de EBS. Las instantáneas se almacenan en Amazon S3. Puede crear un volumen de EBS a partir de una instantánea.

Almacén de instancias

El almacén de instancias ofrece un almacenamiento de nivel de bloques temporal para las instancias. El número, el tamaño y el tipo de volúmenes del almacén de instancias vienen determinados por el tipo y el tamaño de la instancia. Los datos de un volumen del almacén de instancias solo se mantienen durante la vida de la instancia asociada; si una instancia se detiene, se termina o se pone en hibernación, se perderán los datos de los volúmenes del almacén de instancias.

Amazon EFS (solo instancias de Linux)

Amazon EFS proporciona almacenamiento de archivos escalable para su uso con Amazon EC2. Puede crear un sistema de archivos de EFS y configurar las instancias para montar el sistema de archivos. Puede usar un sistema de archivos de EFS como un origen de datos común para aplicaciones y cargas de trabajo que se ejecutan en varias instancias.

Amazon S3

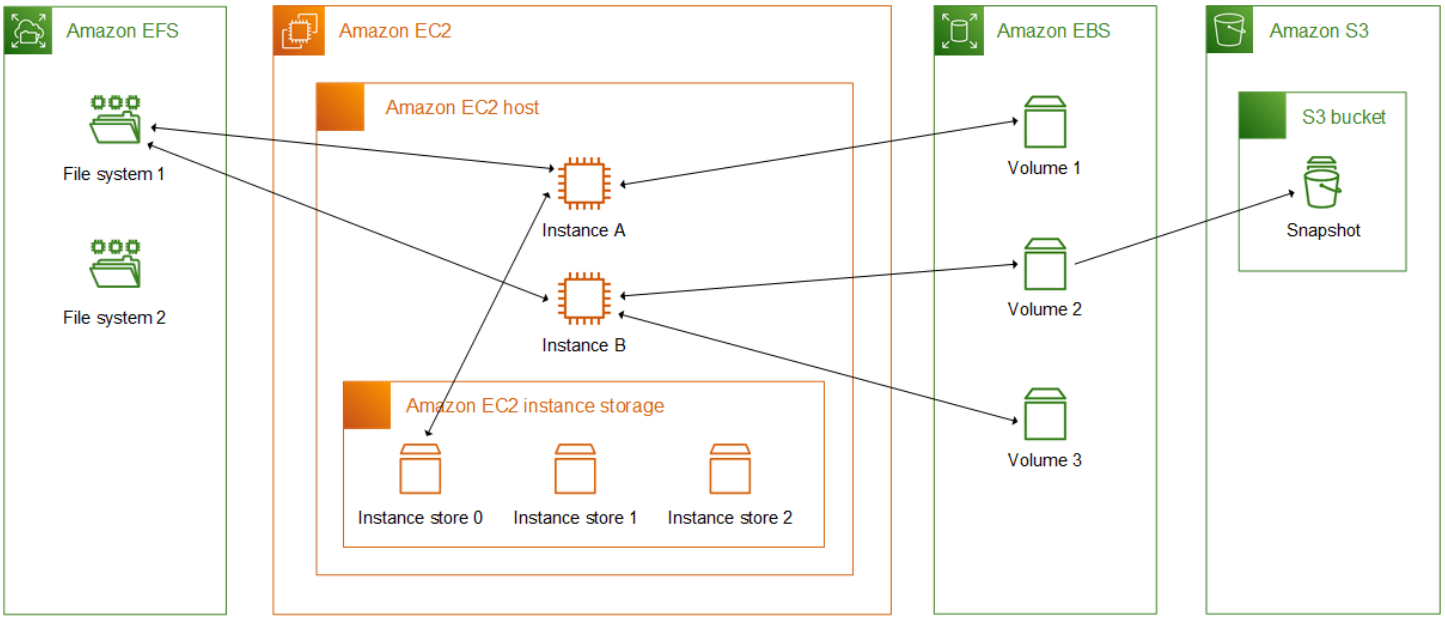
Amazon S3 ofrece acceso a una infraestructura de almacenamiento de datos de confianza y económica. Se ha diseñado para facilitar la computación escalable basada en web, al hacer posible que almacene y recupere cualquier cantidad de datos, en cualquier momento, desde Amazon EC2 o desde cualquier lugar de la web. Por ejemplo, puede utilizar Amazon S3 para

almacenar copias de seguridad de los datos y las aplicaciones. Amazon EC2 utiliza Amazon S3 para almacenar instantáneas de EBS y AMI con respaldo en el almacenamiento de la instancia.

Amazon FSx

Con Amazon FSx, puede iniciar, ejecutar y escalar sistemas de archivos de alto rendimiento con numerosas características en la nube. Amazon FSx es un servicio totalmente administrado que admite una amplia gama de cargas de trabajo. Puede elegir entre estos sistemas de archivos más utilizados: Lustre, NetApp ONTAP, OpenZFS y Windows File Server.

En el siguiente gráfico se muestra la relación entre estas opciones de almacenamiento y su instancia.



Precios de almacenamiento

Abra Precios de AWS, desplácese hasta Precio de los productos de AWS y seleccione Almacenamiento. Elija el producto de almacenamiento para abrir su página de precios.

Uso de Amazon EBS con Amazon EC2

Amazon Elastic Block Store (Amazon EBS) proporciona recursos de almacenamiento en bloque de alto rendimiento y escalables que se pueden utilizar con instancias de Amazon Elastic Compute Cloud (Amazon EC2). Con Amazon EBS, puede crear y administrar los siguientes recursos de almacenamiento en bloque:

- Volúmenes de Amazon EBS: son volúmenes de almacenamiento que se adjuntan a las instancias de Amazon EC2. Después de asociar un volumen a una instancia, puede usarlo de la misma

manera que cualquier otro almacenamiento en bloque. La instancia puede interactuar con el volumen tal y como lo haría con una unidad local.

- Instantáneas de Amazon EBS: son copias de seguridad puntuales de los volúmenes de Amazon EBS que persisten independientemente del volumen en sí. Puede crear instantáneas para hacer una copia de seguridad de los datos en sus volúmenes de Amazon EBS. A continuación, podrá restaurar volúmenes nuevos a partir de esas instantáneas en cualquier momento.

Puede crear y asociar volúmenes de Amazon EBS a una instancia durante la inicialización, y puede crear y asociar volúmenes de EBS a una instancia en cualquier momento después de la inicialización. Y puede crear instantáneas a partir de un volumen en cualquier momento tras su creación.

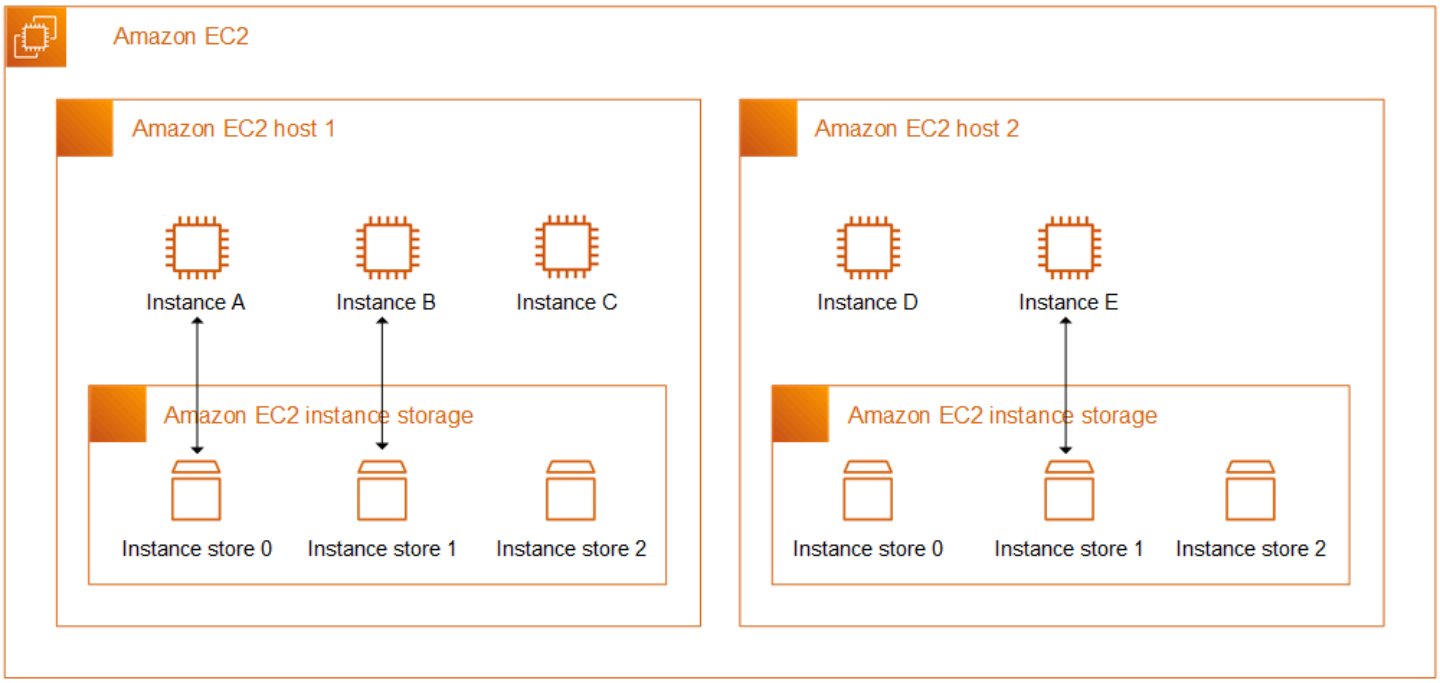
Para obtener más información sobre cómo trabajar con volúmenes e instantáneas, consulte la Guía del usuario de Amazon EBS.

Almacén de instancias Amazon EC2

El almacén de instancias ofrece un almacenamiento de nivel de bloques temporal para la instancia. Este almacenamiento se encuentra en discos que están conectados físicamente al equipo host. El almacén de instancias es ideal para el almacenamiento temporal de información que cambia constantemente, como los búferes, las cachés, los datos de pruebas y otro contenido temporal. También se puede usar para el almacenamiento de datos temporales que se replican en una flota de instancias, como un grupo de servidores web con equilibrio de carga.

Un almacén de instancias consta de uno o varios volúmenes de almacenes de instancias que se exponen como dispositivos de bloques. El tamaño de un almacén de instancias, al igual que el número de dispositivos disponibles, varía por tipo de instancia. Para obtener más información, consulte Volúmenes de almacén de instancias.

Los dispositivos virtuales de los volúmenes de almacenes de instancias son `ephemeral[0-23]`. Los tipos de instancias que admiten un volumen de almacén de instancias tienen `ephemeral0`. Los tipos de instancias que admiten dos volúmenes de almacenes de instancias tienen `ephemeral0` y `ephemeral1`, y así sucesivamente.



Precios de tiendas de instancias

Los volúmenes de almacenes de instancias se incluyen en el costo por uso de la instancia.

Contenido

Volumen de almacén de instancias y vida de los datos

El número, el tamaño y el tipo de volúmenes del almacén de instancias vienen determinados por el tipo y el tamaño de la instancia. Para obtener más información, consulte Volúmenes de almacén de instancias.

Los volúmenes del almacén de instancias solo se adjuntan al iniciar la instancia. No puede adjuntar volúmenes de almacenes de instancias a una instancia después de que la haya iniciado. No puede separar un volumen de almacén de instancias de una instancia y adjuntarlo a otra instancia.

Un volumen de almacén de instancias solo existe durante la vida útil de la instancia a la que está adjunto. No puede configurar un volumen de almacén de instancias para que se mantenga más allá de la vida de la instancia asociada.

Los datos en un volumen de almacén de instancias persisten incluso si la instancia se inicia. Sin embargo, los datos no persisten si la instancia se detiene, hiberna o finaliza. Cuando la instancia se detiene, se termina o se pone en hibernación, cada bloque del volumen del almacén de instancias se elimina de forma criptográfica.

Por lo tanto, no confíe en el almacén de instancias para almacenar datos valiosos a largo plazo. Si necesita retener los datos almacenados en un volumen de almacén de instancias más allá de la vida útil de la instancia, debe copiarlos manualmente a un almacenamiento más persistente, como un volumen de Amazon EBS, un bucket de Amazon S3 o un sistema de archivos de Amazon EFS.

Hay algunos eventos que pueden provocar que los datos no persistan durante toda la vida útil de la instancia. La siguiente tabla indica si los datos de los volúmenes del almacén de instancias se conservan durante eventos específicos, tanto para las instancias virtualizadas como para las instancias bare metal.

Evento	¿Qué ocurre con sus datos?
Eventos del ciclo de vida de las instancias iniciados por el usuario	
La instancia de base de datos se reinicia.	The data persists
La instancia se ha detenido.	The data does not persist
La instancia está hibernando.	The data does not persist
La instancia se termina.	The data does not persist
El tipo del servidor de la instancia de base de datos se ha cambiado	The data does not persist *
Se crea una AMI respaldada por EBS a partir de la instancia	The data does not persist in the created AMI **

Evento	¿Qué ocurre con sus datos?
Crear una AMI desde una instancia con respaldo en el almacén de instancias (Linux instances)	The data persists in the AMI bundle uploaded to Amazon S3 ***
Eventos del sistema operativo iniciados por el usuario	
A shutdown is initiated	The data does not persist †
A restart is initiated	The data persists
Eventos programados de AWS	
Detención de instancia	The data does not persist
Reinicio de la instancia	The data persists
Reinicio del sistema	The data persists
Retirada de instancias	The data does not persist
Eventos no planificados	
Recuperación automática simplificada	The data does not persist
Recuperación basada en acciones de Amazon CloudWatch	The data does not persist
The underlying disk fails	The data on the failed disk does not persist
Power failure	The data persists upon reboot

* Si el nuevo tipo de instancia admite el almacén de instancias, la instancia obtiene la cantidad de volúmenes de almacén de instancias admitidos por el nuevo tipo de instancia, pero los datos no se transfieren a la nueva instancia. Si el nuevo tipo de instancia no admite el almacén de instancias, la instancia no obtiene los volúmenes del almacén de instancias.

** Los datos no se incluyen en la AMI respaldada por EBS ni en los volúmenes del almacén de instancias adjuntos a las instancias iniciadas desde esa AMI.

*** Los datos se incluyen en el paquete de AMI que se carga en Amazon S3. Al iniciar una instancia desde esa AMI, la instancia obtiene los volúmenes del almacén de instancias agrupados en la AMI con los datos que contenían en el momento en que se creó la AMI.

† La protección de terminación y la protección de interrupción no protegen las instancias contra las detenciones o terminaciones de instancias como resultado de los cierres iniciados a través del sistema operativo de la instancia. Los datos almacenados en los volúmenes del almacén de instancias no persisten tanto en los eventos de parada como en los de terminación de instancias.

Volúmenes de almacén de instancias

El número, el tamaño y el tipo de volúmenes del almacén de instancias vienen determinados por el tipo y el tamaño de la instancia. Algunos tipos de instancias, como M6, C6 y R6, no admiten volúmenes de almacén de instancias, mientras que otros tipos de instancias, como M5d, C6gd y R6gd, sí admiten volúmenes de almacén de instancias. No puedes adjuntar más volúmenes de almacén de instancias a una instancia de los que admite su tipo de instancia. Para los tipos de instancia que admiten volúmenes de almacén de instancias, el número y el tamaño de los volúmenes de almacén de instancias varían en función del tamaño de la instancia Por ejemplo, `m5d.large` admite 1 volumen de almacén de instancias de 75 GB, mientras que `m5d.24xlarge` admite 4 volúmenes de almacén de instancias de 900 GB.

En el caso de los tipos de instancias con volúmenes de almacén de instancias de NVMe, todos los volúmenes de almacenes de instancias compatibles se adjuntan automáticamente a la instancia en el momento de la inicialización. Para los tipos de instancias con volúmenes de almacén de instancias que no sean de NVMe, como C1, C3, M1, M2, M3, R3, D2, H1, I2, X1 y X1e, debe especificar manualmente las asignaciones de dispositivos de bloque para los volúmenes del almacén de instancia que desea adjuntar en el momento de la inicialización. Luego, una vez iniciada la instancia, debes formatear y montar los volúmenes del almacén de instancias adjuntos antes de poder usarlos. No puede hacer que un volumen de almacén de instancias esté disponible después de iniciar la instancia.

Algunos tipos de instancias utilizan unidades de estado sólido (SSD) basadas en NVMe o SATA, mientras que otros utilizan unidades de disco duro (HDD) basadas en SATA. Esta opción es recomendable cuando necesita almacenamiento con una latencia muy baja, pero no necesita que los datos se conserven cuando termina la instancia, o bien puede utilizar arquitecturas tolerantes a errores. Para obtener más información, consulte Volúmenes de almacén de instancias SSD.

Los datos de los volúmenes de almacén de instancias de NVMe y algunos volúmenes de almacén de instancias de HDD se cifran en reposo. Para obtener más información, consulte Proteger los datos en Amazon EC2.

Volúmenes de almacén de instancias disponibles

En la Guía de tipos de instancias de Amazon EC2 se incluye la cantidad, el tamaño, el tipo y las optimizaciones de rendimiento de los volúmenes de almacenes de instancias que hay disponibles en cada tipo de instancia admitido. Para más información, consulte los siguientes temas:

- Especificaciones del almacén de instancias: uso general
- Especificaciones del almacén de instancias: optimizadas para la computación
- Especificaciones del almacén de instancias: memoria optimizada
- Especificaciones del almacén de instancias: almacenamiento optimizado
- Especificaciones del almacén de instancias: computación acelerada
- Especificaciones del almacén de instancias: computación de alto rendimiento
- Especificaciones del almacén de instancias: generación anterior

Cómo recuperar la información de volumen del almacén de instancias mediante la AWS CLI

Puede utilizar el comando de la AWS CLI describe-instance-types para mostrar información sobre un tipo de instancias, como sus volúmenes de almacén de instancias. En el ejemplo siguiente se muestra el tamaño total del almacenamiento de instancias para todas las instancias R5 con volúmenes de almacén de instancias.

```
aws ec2 describe-instance-types \
    --filters "Name=instance-type,Values=r5*" "Name=instance-storage-
supported,Values=true" \
    --query "InstanceTypes[].[InstanceType, InstanceStorageInfo.TotalSizeInGB]" \
    --output table
```

Ejemplo de resultado

```
--------------------------
|  DescribeInstanceTypes  |
+----------------+--------+
|  r5ad.24xlarge |  3600  |
|  r5ad.12xlarge |  1800  |
|  r5dn.8xlarge  |  1200  |
```

```
|  r5ad.8xlarge  |  1200  |
|  r5ad.large    |  75    |
|  r5d.4xlarge   |  600   |
   . . .
|  r5dn.2xlarge  |  300   |
|  r5d.12xlarge  |  1800  |
+----------------+--------+
```

En el ejemplo siguiente se muestran los detalles completos de almacenamiento de instancias para el tipo de instancias especificado.

```
aws ec2 describe-instance-types \
    --filters "Name=instance-type,Values=r5d.4xlarge" \
    --query "InstanceTypes[].InstanceStorageInfo"
```

El resultado del ejemplo muestra que este tipo de instancias tiene dos volúmenes SSD NVMe de 300 GB, lo que supone un total de 600 GB de almacenamiento de instancias.

```
[
    {
        "TotalSizeInGB": 600,
        "Disks": [
            {
                "SizeInGB": 300,
                "Count": 2,
                "Type": "ssd"
            }
        ],
        "NvmeSupport": "required"
    }
]
```

Cómo agregar volúmenes de almacén de instancias a la instancia de EC2

En el caso de los tipos de instancias con volúmenes de almacén de instancias de NVMe, todos los volúmenes de almacenes de instancias compatibles se adjuntan automáticamente a la instancia en el momento del lanzamiento. Los volúmenes de almacén de instancias NVMe se enumeran automáticamente y se les asigna un nombre de dispositivo.

Para los tipos de instancias con volúmenes de almacén de instancias que no sean de NVMe, como C1, C3, M1, M2, M3, R3, D2, H1, I2, G2, X1 y X1e, debe especificar manualmente las asignaciones

de dispositivos de bloques para los volúmenes del almacén de instancias que desea adjuntar en el momento de la inicialización. Las asignaciones de dispositivos de bloques se pueden especificar en la solicitud de inicialización de la instancia o en la AMI utilizada para iniciar la instancia. Cada entrada de una asignación de dispositivos de bloques incluye un nombre de dispositivo y el volumen al que se mapea. Para obtener más información, consulte Mapeos de dispositivos de bloques

> **Important**
>
> Solo puede especificar volúmenes de almacenes de instancias al iniciar la instancia. No puede adjuntar volúmenes de almacenes de instancias a una instancia después de que la haya iniciado.

Después de iniciar una instancia, debe asegurarse de que los volúmenes de almacenes de instancias de su instancia están formateados y montados antes de usarlos. El volumen raíz de una instancia con respaldo en un almacén de instancias se monta automáticamente.

Consideración de los volúmenes raíz

Un mapeo de dispositivos de bloques siempre especifica el volumen raíz de la instancia. El volumen raíz se monta siempre automáticamente.

Instancias de Linux: el volumen raíz es un volumen de Amazon EBS o un volumen de almacén de instancias. Para instancias con un volumen de almacén de instancias para el volumen raíz, el tamaño de este volumen varía por AMI, pero el tamaño máximo es 10 GB. Para obtener más información, consulte Almacenamiento para el dispositivo raíz.

Instancias de Windows: el volumen raíz debe ser un volumen de Amazon EBS. No se admite el almacén de instancias para el volumen raíz.

Contenido

Agregar volúmenes de almacén de instancias a una AMI

Puede crear una AMI con una asignación de dispositivos de bloques que incluya volúmenes de almacenes de instancias.

Si inicia una instancia que admite volúmenes de almacén de instancias que no son NVMe mediante una AMI que especifica asignaciones de dispositivos de bloque de volumen de almacén de instancias, la instancia incluye los volúmenes de almacén de instancias. Si el número de volúmenes de almacén de instancias en la asignación de dispositivo de bloque excede el número de volúmenes de almacén de instancias disponible para la instancia, los volúmenes adicionales de almacén de instancias se ignoran.

Si inicia una instancia que admite volúmenes de almacén de instancias de NVMe mediante una AMI que especifica las asignación de dispositivos de bloque de volumen de almacén de instancias, se ignoran las asignación de dispositivos de bloque de volumen del almacén de instancias. Las instancias que admiten los volúmenes de almacenes de instancias de NVMe obtienen todos sus volúmenes de almacén de instancias compatibles, independientemente de las asignaciones de dispositivos de bloques especificadas en la solicitud de inicialización de instancias y en la AMI.

Consideraciones

- Para las instancias M3, especifique los volúmenes del almacén de instancias en la asignación de dispositivos de bloques de la instancia, no de la AMI. Amazon EC2 podría ignorar los volúmenes del almacén de instancias que solo se especifican en la asignación de dispositivos de bloques de la AMI.
- Cuando inicia una instancia, puede omitir los volúmenes de almacén de instancias que no sean NVMe especificados en la asignación de dispositivos de bloques de AMI o añadir volúmenes de almacén de instancias.

New console

Para añadir volúmenes de almacenes de instancias a una AMI basada en Amazon EBS con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instancias y seleccione la instancia.
3. Elija Acciones, Imagen y plantillas, Crear imagen.
4. En el cuadro de diálogo Crear imagen, escriba un nombre significativo y una descripción para la imagen.
5. Por cada volumen de almacén de instancias que vaya a agregar, elija Agregar volumen, en Tipo de volumen seleccione un volumen de almacén de instancias y en Dispositivo seleccione un nombre de dispositivo. (Para obtener más información, consulte Nombres de

dispositivos en las instancias de Amazon EC2). El número de volúmenes de almacenes de instancias disponibles depende del tipo de instancia. Para las instancias con volúmenes de almacenes de instancias NVMe, el mapeo de dispositivos de estos volúmenes depende del orden en el que el sistema operativo enumere los volúmenes.

6. Elija Crear imagen.

AWS CLI

Para añadir volúmenes de almacenes de instancias a una AMI utilizando la línea de comandos

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

- create-image o register-image (AWS CLI)
- New-EC2Image y Register-EC2Image (AWS Tools for Windows PowerShell)

Agregar volúmenes de almacén de instancias a una instancia

Cuando inicia una instancia que admite volúmenes de almacén de instancias que no son NVMe, debe especificar asignaciones de dispositivos de bloque para que se adjunten los volúmenes de almacén de instancias. Las asignaciones de dispositivos de bloques deben especificarse en la solicitud de inicialización de la instancia o en la AMI utilizada para iniciar la instancia.

Si la AMI incluye asignaciones de dispositivos de bloques para los volúmenes del almacén de instancias, no es necesario que especifique las asignaciones de dispositivos en bloque en la solicitud de inicialización de la instancia, a menos que necesite más volúmenes de almacén de instancias de los que se incluyen en la AMI.

Si la AMI no incluye las asignaciones de dispositivos de bloque para los volúmenes de almacén de instancias, debe especificar las asignaciones de dispositivos de bloque en la solicitud de inicialización de la instancia.

Consideraciones

- Para instancias M3, podría recibir volúmenes de almacenes de instancias aunque no las especifique en la asignación de dispositivos de bloques para la instancia.

Para especificar las asignaciones de dispositivos de bloques en la solicitud de inicialización de la instancia, utilice uno de los métodos siguientes.

Amazon EC2 console

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel, elija Iniciar instancia.
3. En la sección Imágenes de aplicaciones y sistema operativo, seleccione la AMI que desea utilizar.
4. En la sección Configurar almacenamiento, la sección Volúmenes de almacén de instancias muestra los volúmenes del almacén de instancias que se pueden adjuntar a la instancia. El número de volúmenes de almacén de instancias disponibles depende del tipo de instancia.
5. Para cada volumen de almacén de instancias que desee adjuntar, en Nombre del dispositivo, seleccione el nombre del dispositivo que desee utilizar.
6. Configure los ajustes de inicialización de instancias restantes según sea necesario y luego escoja Iniciar instancia.

Command line

Puede usar uno de estos comandos con la opción correspondiente.

- `--block-device-mappings` con run-instances (AWS CLI)
- `-BlockDeviceMapping` con New-EC2Instance (AWS Tools for Windows PowerShell)

Hacer que los volúmenes de almacén de instancias estén disponibles en la instancia

Tras iniciar una instancia con volúmenes de almacén de instancias adjuntos, debe montarlos antes de poder acceder a ellos.

> **Note**
>
> Muchos volúmenes de almacenes de instancias están formateados previamente con el sistema de archivos ext3. Los volúmenes de almacenes de instancias basados en SSD que admiten la instrucción TRIM no están formateados previamente con ningún sistema de archivos. Sin embargo, puede formatear volúmenes con el sistema de archivos que elija después de iniciar la instancia. Para obtener más información, consulte Soporte TRIM del

volumen de almacén de instancias. En el caso de las instancias de Windows, reformateamos los volúmenes de almacenes de instancias con el sistema de archivos NTFS.

instancias de Linux

Puede ver y montar los volúmenes de almacén de instancias tal y como se describe en el siguiente procedimiento.

Para hacer que un volumen de almacén de instancias esté disponible en Linux

1. Conéctese a la instancia utilizando un cliente SSH. Para obtener más información, consulte Conexión con la instancia de Linux.
2. Utilice el comando `df -h` para ver los volúmenes que están formateados y montados.

```
$ df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        3.8G   72K  3.8G   1% /dev
tmpfs           3.8G     0  3.8G   0% /dev/shm
/dev/nvme0n1p1  7.9G  1.2G  6.6G  15% /
```

3. Utilice `lsblk` para ver los volúmenes que se han mapeado en la inicialización, pero no están formateados ni montados.

```
$ lsblk
NAME          MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
nvme0n1       259:1    0    8G  0 disk
##nvme0n1p1   259:2    0    8G  0 part /
##nvme0n1p128 259:3    0    1M  0 part
nvme1n1       259:0    0 69.9G  0 disk
```

4. Para formatear y montar un volumen de almacén de instancias que solo se ha asignado, haga lo siguiente:

   a. Cree un sistema de archivos en el dispositivo utilizando el comando `mkfs`.

   ```
   $ sudo mkfs -t xfs /dev/nvme1n1
   ```

   b. Cree un directorio en el que montar el dispositivo utilizando el comando `mkdir`.

```
$ sudo mkdir /data
```

c. Monte el dispositivo en el directorio recién creado utilizando el comando `mount`.

```
$ sudo mount /dev/nvme1n1 /data
```

instancias de Windows

También puede ver los volúmenes de almacén de instancias utilizando la administración de discos de Windows. Para obtener más información, consulte Listar discos utilizando Disk Management.

Para montar manualmente un volumen de almacén de instancias

1. Elija Inicio, escriba Administración de equipos, y, a continuación, pulse Intro.
2. En el panel izquierdo, elija Administración de discos.
3. Si se le pide que inicialice el volumen, elija el volumen que desea inicializar, seleccione el tipo de partición requerido según su caso de uso y, a continuación, elija Aceptar.
4. En la lista de volúmenes, haga clic con el botón secundario en el volumen que desea montar y, a continuación, elija Nuevo volumen simple.
5. En el asistente, elija Siguiente.
6. En la pantalla Especificar tamaño de volumen, elija Siguiente para utilizar el tamaño máximo del volumen. Como opción, elija un tamaño de volumen que esté entre el espacio mínimo y el máximo en disco.
7. En la pantalla Asignar una letra de unidad o ruta de acceso, realice una de las siguientes acciones y elija Siguiente.
   - Para montar el volumen con una letra de unidad, elija Asignar la siguiente letra de unidad y, a continuación, elija la letra de unidad que desee utilizar.
   - Para montar el volumen como carpeta, elija Montar en la siguiente carpeta NTFS vacía y, a continuación, elija Examinar para crear o seleccionar la carpeta que desea utilizar.
   - Para montar el volumen sin una letra de unidad o ruta de acceso, elija No asignar una letra de unidad o ruta de unidad.
8. En la pantalla Formato de partición, especifique si desea dar formato o no al volumen. Si elige dar formato al volumen, elija el sistema de archivos y el tamaño de unidad necesarios y especifique una etiqueta de volumen.

9. Elija Siguiente, Finalizar.

Para obtener instrucciones sobre cómo montar un volumen asociado automáticamente después de reiniciar, consulte Cómo montar automáticamente un volumen asociado después de reiniciar en la Guía del usuario de Amazon EBS.

Volúmenes de almacén de instancias SSD

Al igual que otros volúmenes de almacén de instancias, debe mapear los volúmenes de almacén de instancias SSD para la instancia cuando la lance. Los datos de un volumen de instancias SSD persisten únicamente durante la vida de su instancia de asociada. Para obtener más información, consulte Cómo agregar volúmenes de almacén de instancias a la instancia de EC2.

Volúmenes SSD de NVMe

Algunas instancias ofrecen volúmenes de almacenes de instancias SSD (unidades de estado sólido) de memoria rápida no volátil (NVMe). Para obtener más información sobre el tipo de volumen de almacén de instancias admitido por cada tipo de instancia, consulte Volúmenes de almacén de instancias.

Los datos incluidos en el almacenamiento de instancias de NVMe se cifran mediante un cifrado de bloques XTS-AES-256 en un módulo de hardware de la instancia. Las claves de cifrado se generan mediante el módulo de hardware y son únicas para cada dispositivo de almacenamiento de instancias de NVMe. Todas las claves de cifrado se destruyen cuando se detiene o termina la instancia y no se pueden recuperar. No puede deshabilitar este cifrado ni tampoco proporcionar su propia clave de cifrado.

instancias de Linux

Para obtener acceso a los volúmenes NVMe, deben estar instalados los controladores NVMe. Las AMI siguientes cumplen este requisito:

- AL2023
- Amazon Linux 2
- AMI de Amazon Linux 2018.03 y posterior
- Ubuntu 14.04 o versiones posteriores con el kernel `linux-aws`

> **Note**
>
> Los tipos de instancias basados en AWS Graviton requieren Ubuntu 18.04 o versiones posteriores con kernel `linux-aws`

- Red Hat Enterprise Linux 7.4 o versiones posteriores
- SUSE Linux Enterprise Server 12 SP2 o versiones posteriores
- CentOS 7.4.1708 o versiones posteriores
- FreeBSD 11.1 o versiones posteriores
- Debian GNU/Linux 9 o versiones posteriores

- Bottlerocket

Después de conectarse a la instancia, puede ver una lista de los dispositivos NVMe utilizando el comando lspci. A continuación, se muestra una salida de ejemplo de una instancia `i3.8xlarge`, que admite cuatro dispositivos NVMe.

```
[ec2-user ~]$ lspci
00:00.0 Host bridge: Intel Corporation 440FX - 82441FX PMC [Natoma] (rev 02)
00:01.0 ISA bridge: Intel Corporation 82371SB PIIX3 ISA [Natoma/Triton II]
00:01.1 IDE interface: Intel Corporation 82371SB PIIX3 IDE [Natoma/Triton II]
00:01.3 Bridge: Intel Corporation 82371AB/EB/MB PIIX4 ACPI (rev 01)
00:02.0 VGA compatible controller: Cirrus Logic GD 5446
00:03.0 Ethernet controller: Device 1d0f:ec20
00:17.0 Non-Volatile memory controller: Device 1d0f:cd01
00:18.0 Non-Volatile memory controller: Device 1d0f:cd01
00:19.0 Non-Volatile memory controller: Device 1d0f:cd01
00:1a.0 Non-Volatile memory controller: Device 1d0f:cd01
00:1f.0 Unassigned class [ff80]: XenSource, Inc. Xen Platform Device (rev 01)
```

Si utiliza un sistema operativo compatible, pero no ve los dispositivos NVMe, compruebe que el módulo NVMe esté cargado utilizando el comando siguiente.

- Amazon Linux, Amazon Linux 2, Ubuntu 14/16, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, CentOS 7

```
$ lsmod | grep nvme
```

```
nvme           48813  0
```

- Ubuntu 18

```
$ cat /lib/modules/$(uname -r)/modules.builtin | grep nvme
s/nvme/host/nvme-core.ko
kernel/drivers/nvme/host/nvme.ko
kernel/drivers/nvmem/nvmem_core.ko
```

Los volúmenes NVMe son compatibles con la especificación NVMe 1.0e. Puede utilizar comandos NVMe con los volúmenes NVMe. Con Amazon Linux, puede instalar el paquete `nvme-cli` desde el repositorio utilizando el comando yum install. Con otras versiones soportadas de Linux, puede descargar el paquete `nvme-cli` si no está disponible en la imagen.

instancias de Windows

Las AMI para Windows de AWS más recientes de los siguientes sistemas operativos Windows contienen los controladores NVMe de AWS utilizados para interactuar con los volúmenes del almacén de instancias de SSD que se exponen como dispositivos de bloques NVMe para un mejor rendimiento:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

Después de conectarse a la instancia, puede verificar que ve los volúmenes NVMe en el administrador de discos. En la barra de tareas, abra el menú contextual (haga clic con el botón derecho) del logotipo de Windows y elija Administración de discos.

Las AMI para Windows de AWS proporcionadas por Amazon incluyen el controlador NVMe de AWS. Si no está utilizando las AMI de Windows de AWS más recientes, instale el controlador NVMe de AWS actual.

Volúmenes SSD sin NVMe

Las siguientes instancias admiten volúmenes de almacén de instancias que utilizan unidades de estado sólido que no son de NVMe para ofrecer un alto rendimiento de E/S de asignación al azar:

C3, I2, M3, R3 y X1. Para obtener más información acerca de los volúmenes de almacenes de instancias que admite cada tipo de instancia, consulte Volúmenes de almacén de instancias.

Rendimiento de E/S del volumen de almacén de instancias basado en SSD

A medida que llena los volúmenes de almacén de instancias basadas en SSD para la instancia, disminuye el número de IOPS de escritura que se pueden obtener. Esto se debe al trabajo adicional que debe realizar el controlador SSD para encontrar espacio disponible, volver a escribir los datos existentes y borrar el espacio no utilizado para que se pueda volver a escribir. Este proceso de recopilación de elementos no utilizados genera una amplificación de escritura interna en el SSD, expresada como ratio de operaciones de escritura de SSD con respecto a las operaciones de escritura del usuario. Este descenso del rendimiento es aún mayor si las operaciones de escritura no están en múltiplos de 4096 bytes o no están alineadas con un límite de 4096 bytes. Si escribe una cantidad más pequeña de bytes o bytes que no están alineados, el controlador SSD debe leer los datos circundantes y almacenar el resultado en una nueva ubicación. Este patrón genera una amplificación de escritura significativamente mayor, una mayor latencia y se reduce en gran medida el rendimiento de E/S.

Los controladores SSD pueden utilizar varias estrategias para reducir el impacto de la amplificación de escritura. Una de estas estrategias es reservar espacio en el almacén de instancias SSD para que el controlador pueda administrar con más eficiencia el espacio disponible para las operaciones de escritura. Esto se llama aprovisionamiento excesivo. Los volúmenes de almacén de instancias basadas en SSD proporcionados para una instancia no tienen espacio reservado para el aprovisionamiento excesivo. Para reducir la amplificación de escritura, recomendamos dejar un 10 % del volumen sin particiones, de modo que el controlador SSD pueda utilizarlo para el aprovisionamiento excesivo. Esto reduce el almacenamiento que se puede utilizar, pero aumenta el rendimiento aunque el disco esté a punto de llegar a su capacidad máxima.

Para los volúmenes de almacén de instancias que admiten TRIM, puede utilizar el comando TRIM para notificar al controlador SSD cuando deje de necesitar los datos que ha escrito. Esto aporta al controlador más espacio libre, lo que puede reducir la amplificación de escritura y aumentar el rendimiento. Para obtener más información, consulte Soporte TRIM del volumen de almacén de instancias.

Soporte TRIM del volumen de almacén de instancias

Algunos tipos de instancias admiten volúmenes SSD con TRIM. Para obtener más información, consulte Volúmenes de almacén de instancias.

> **Note**
>
> (Solo instancias de Windows) Las instancias que ejecutan Windows Server 2012 R2 admiten TRIM a partir de la versión 7.3.0 del controlador PV de AWS. Las instancias que ejecutan versiones anteriores de Windows Server no admiten TRIM.

Los volúmenes de almacenes de instancias que admiten TRIM se recortan por completo antes de asignarlos a la instancia. Estos volúmenes no están formateados con un sistema de archivos cuando se inicia una instancia, por lo que debe formatearlos antes de montarlos y usarlos. Para obtener acceso más rápidamente a estos volúmenes, debería omitir la operación TRIM cuando los formatee.

(Instancias de Windows) Para desactivar temporalmente la compatibilidad con TRIM durante el formateo inicial, use el comando `fsutil behavior set DisableDeleteNotify 1`. Una vez completado el formateo, vuelva a habilitar la compatibilidad con TRIM mediante `fsutil behavior set DisableDeleteNotify 0`.

Con volúmenes de almacenes de instancias que admiten TRIM, puede utilizar el comando TRIM para notificar al controlador SSD cuando deje de necesitar los datos que ha escrito. Esto aporta al controlador más espacio libre, lo que puede reducir la amplificación de escritura y aumentar el rendimiento. En las instancias de Linux, utilice el comando `fstrim` para habilitar el TRIM periódico. En las instancias de Windows, utilice el comando `fsutil behavior set DisableDeleteNotify 0` para asegurarse de que la compatibilidad con TRIM esté habilitada durante el funcionamiento normal.

Volúmenes de intercambio de almacén de instancias para instancias de Linux

> **Note**
>
> Este tema se aplica a las instancias de Linux únicamente.

El espacio de intercambio en Linux puede utilizarse cuando un sistema necesita más memoria que la que tiene asignada físicamente. Cuando se habilita el espacio de intercambio, los sistemas Linux pueden intercambiar páginas de memoria que se utilizan con poca frecuencia de la memoria física al espacio de intercambio (una partición especial o un archivo de intercambio en un sistema de archivos existente) y liberar ese espacio para las páginas de memoria que requieren acceso de alta velocidad.

> **Note**
>
> El uso del espacio de intercambio para las páginas de memoria no es tan rápido ni eficiente como utilizar RAM. Si la carga de trabajo pagina memoria con regularidad en el espacio de intercambio, debería pensar en la posibilidad de migrarlo a un tipo de instancia de mayor tamaño con más RAM. Para obtener más información, consulte Cambie el tipo de instancia.

Los tipos de instancias `c1.medium` y `m1.small` tienen una cantidad limitada de memoria física con la que trabajar, y disponen de un volumen de intercambio de 900 MiB durante su inicialización para actuar como memoria virtual para las AMIs de Linux. Aunque el kernel de Linux considera este espacio de intercambio como una partición en el dispositivo raíz, en realidad es un volumen de almacén de instancias distinto, sin importar el tipo de dispositivo raíz.

Amazon Linux habilita y utiliza automáticamente este espacio de intercambio, pero es posible que la AMI necesite algunos pasos adicionales para reconocer y utilizar este espacio de intercambio. Para comprobar si la instancia utiliza el espacio de intercambio, puede utilizar el comando swapon -s.

```
[ec2-user ~]$ swapon -s
Filename                                Type            Size    Used    Priority
/dev/xvda3                              partition       917500  0       -1
```

La instancia anterior tiene adjuntado y habilitado un volumen de intercambio de 900 MiB. Si no ve un volumen de intercambio con este comando, es posible que tenga que habilitar el espacio de intercambio del dispositivo. Para comprobar los discos disponibles, utilice el comando lsblk.

```
[ec2-user ~]$ lsblk
NAME  MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda1 202:1    0    8G  0 disk /
xvda3 202:3    0  896M  0 disk
```

Aquí, está disponible el volumen de intercambio `xvda3` para la instancia, pero no está habilitado (fíjese en que el campo `MOUNTPOINT` está vacío). Puede habilitar el volumen de intercambio con el comando swapon.

> **Note**
>
> Tiene que colocar `/dev/` como prefijo en el nombre del dispositivo que aparece con el comando lsblk. Es posible que su dispositivo tenga otro nombre, como `sda3`, `sde3` o `xvde3`. Utilice el nombre de dispositivo de su sistema en el siguiente comando.

```
[ec2-user ~]$ sudo swapon /dev/xvda3
```

Ahora, el espacio de intercambio debería aparecer en la salida de lsblk y swapon -s.

```
[ec2-user ~]$ lsblk
NAME  MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda1 202:1    0    8G  0 disk /
xvda3 202:3    0  896M  0 disk [SWAP]
[ec2-user ~]$ swapon -s
Filename                                Type            Size    Used    Priority
/dev/xvda3                              partition       917500  0       -1
```

También tiene que editar el archivo `/etc/fstab` para que este espacio de intercambio se habilite automáticamente en cada arranque del sistema.

```
[ec2-user ~]$ sudo vim /etc/fstab
```

Adjunte la siguiente línea al archivo `/etc/fstab` (utilizando el nombre del dispositivo de intercambio del sistema):

```
/dev/xvda3       none    swap    sw  0       0
```

Para utilizar un volumen de almacén de instancias como espacio de intercambio

Se puede utilizar cualquier volumen de almacén de instancias como espacio de intercambio. Por ejemplo, el tipo de instancia `m3.medium` incluye un volumen de almacén de instancias SSD de 4 GB que es apropiado para el espacio de intercambio. Si el volumen de almacén de instancias es mucho mayor (por ejemplo, 350 GB), puede pensar en la posibilidad de particionar el volumen con una partición de intercambio menor de 4-8 GB y el resto para un volumen de datos.

> **Note**
>
> Este procedimiento solo se aplica a los tipos de instancias que admiten el almacenamiento de instancias. Para ver una lista de los tipos de instancia admitidos, consulte Volúmenes de almacén de instancias.

1. Muestre los dispositivos de bloques adjuntados a la instancia para obtener el nombre de dispositivo del volumen de almacén de instancias.

```
[ec2-user ~]$ lsblk -p
NAME       MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
/dev/xvdb  202:16   0   4G  0 disk /media/ephemeral0
/dev/xvda1 202:1    0   8G  0 disk /
```

   En este ejemplo, el volumen de almacén de instancias es `/dev/xvdb`. Dado que se trata de una instancia de Amazon Linux, el volumen de almacén de instancias se formatea y se monta en `/media/ephemeral0`, aunque no todos los sistemas operativos Linux hacen esto automáticamente.

2. (Opcional) Si el volumen de almacén de instancias está montado (muestra un `MOUNTPOINT` en la salida del comando lsblk), tiene que desmontarlo con el siguiente comando.

```
[ec2-user ~]$ sudo umount /dev/xvdb
```

3. Configure un área de intercambio de Linux en el dispositivo mediante el comando mkswap.

```
[ec2-user ~]$ sudo mkswap /dev/xvdb
mkswap: /dev/xvdb: warning: wiping old ext3 signature.
Setting up swapspace version 1, size = 4188668 KiB
no label, UUID=b4f63d28-67ed-46f0-b5e5-6928319e620b
```

4. Habilite el espacio de intercambio.

```
[ec2-user ~]$ sudo swapon /dev/xvdb
```

5. Compruebe que el nuevo espacio de intercambio se está utilizando.

```
[ec2-user ~]$ swapon -s
Filename    Type  Size Used Priority
```

```
/dev/xvdb                                 partition 4188668 0 -1
```

6. Edite el archivo `/etc/fstab` para que este espacio de intercambio se habilite automáticamente en cada arranque del sistema.

   ```
   [ec2-user ~]$ sudo vim /etc/fstab
   ```

   Si el archivo `/etc/fstab` tiene una entrada para `/dev/xvdb` (o `/dev/sdb`), cámbiela para que se corresponda con la siguiente línea; si no tiene una entrada para este dispositivo, adjunte la siguiente línea al archivo `/etc/fstab` (utilizando el nombre del dispositivo de intercambio del sistema):

   ```
   /dev/xvdb       none    swap    sw  0       0
   ```

   Important

   Los datos de los volúmenes del almacén de instancias se pierden cuando una instancia se detiene o hiberna; esto incluye el formato del espacio de intercambio de almacenes de instancias creado en Step 3. Si detiene y reinicia una instancia que se ha configurado para utilizar el espacio de intercambio del almacén de instancias, debe repetir Step 1 a Step 5 en el nuevo volumen de almacén de instancias.

Optimización del desempeño del disco para los volúmenes de almacén de instancias en instancias de Linux

Note

Este tema se aplica a las instancias de Linux únicamente.

Debido al modo en que Amazon EC2 virtualiza los discos, la primera escritura en cualquier ubicación en algunos volúmenes de almacenes de instancias se realiza a menor velocidad que las escrituras siguientes. Para la mayoría de las aplicaciones, la amortización de este costo a lo largo de la vida útil de la instancia es aceptable. Sin embargo, si necesita un alto rendimiento del disco, le recomendamos que inicialice sus unidades escribiendo una vez en cada ubicación de unidad antes de su uso en producción.

> **Note**
>
> Algunos tipos de instancias con soporte de unidades de estado sólido (SSD) conectadas directamente y TRIM ofrecen el rendimiento máximo en la inicialización, sin inicialización. Para obtener más información acerca del almacén de instancia para cada tipo de instancia, consulte Volúmenes de almacén de instancias.

Si necesita más flexibilidad en latencia o rendimiento, es recomendable utilizar Amazon EBS.

Para inicializar los volúmenes de almacenes de instancias, utilice los siguientes comandos dd según el almacén que desee inicializar (por ejemplo, `/dev/sdb` o `/dev/nvme1n1`).

> **Note**
>
> Asegúrese de desmontar la unidad antes de utilizar este comando.
> La inicialización puede llevar mucho tiempo (unas 8 horas para una instancia extragrande).

Para inicializar los volúmenes de almacenes de instancias, utilice los siguientes comandos en los tipos de instancias `m1.large`, `m1.xlarge`, `c1.xlarge`, `m2.xlarge`, `m2.2xlarge` y `m2.4xlarge`:

```
dd if=/dev/zero of=/dev/sdb bs=1M
dd if=/dev/zero of=/dev/sdc bs=1M
dd if=/dev/zero of=/dev/sdd bs=1M
dd if=/dev/zero of=/dev/sde bs=1M
```

Para realizar la inicialización en todos los volúmenes de almacenes de instancias al mismo tiempo, utilice el siguiente comando:

```
dd if=/dev/zero bs=1M|tee /dev/sdb|tee /dev/sdc|tee /dev/sde > /dev/sdd
```

Al configurar las unidades para RAID, estas se inicializan escribiendo en cada ubicación de las unidades. Al configurar la RAID basada en software, asegúrese de cambiar la velocidad de reconstrucción mínima:

```
echo $((30*1024)) > /proc/sys/dev/raid/speed_limit_min
```

Almacenamiento de archivos

El almacenamiento de archivos en la nube es un método para almacenar datos en la nube que suministra a servidores y aplicaciones acceso a los datos mediante sistemas de archivos compartidos. Esta compatibilidad hace que el almacenamiento de archivos en la nube sea ideal para las cargas de trabajo que dependen de sistemas de archivos compartidos y provee una integración simple sin necesidad de introducir cambios en el código.

Existen numerosas soluciones de almacenamiento de archivos, desde un servidor de archivos de nodo único en una instancia informática que utiliza el almacenamiento de bloques como base sin escalabilidad o pocas redundancias para proteger los datos, hasta una solución en clúster autoadministrada o una solución completamente administrada. El contenido que se muestra a continuación, presenta una introducción a algunos de los servicios de almacenamiento proporcionados por AWS para su uso con instancias de Amazon EC2.

Contenido

Usar Amazon S3 con Amazon EC2

Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos que ofrece escalabilidad, disponibilidad de datos, seguridad y rendimiento líderes del sector. Puede usar Amazon S3 para almacenar y recuperar cualquier cantidad de datos para varios casos de uso, como lagos de datos, sitios web, copias de seguridad y análisis de macrodatos, desde una instancia de Amazon EC2 o desde cualquier lugar de Internet. Para obtener más información, consulte ¿Qué es Amazon S3?

Los objetos son las entidades fundamentales almacenadas en Amazon S3. Todos los objetos almacenados en Amazon S3 están dentro de un bucket. Los buckets organizan el espacio de nombres de Amazon S3 en el nivel más alto e identifican la cuenta responsable de ese almacenamiento. Los buckets de Amazon S3 son similares a los nombres de dominios de Internet. Los objetos almacenados en los buckets poseen un valor de clave único y se recuperan utilizando una dirección URL. Por ejemplo, si un objeto con el valor clave `/photos/mygarden.jpg` se

almacena en el bucket `DOC-EXAMPLE-BUCKET1`, es direccionable mediante la URL `https://DOC-EXAMPLE-BUCKET1.s3.amazonaws.com/photos/mygarden.jpg`. Para obtener más información, consulte Cómo funciona Amazon S3.

Ejemplos de uso

Dados los beneficios que tiene Amazon S3 para el almacenamiento, es posible que desee utilizar este servicio para almacenar archivos y conjuntos de datos para utilizarlos con instancias de EC2. Hay varias formas de mover datos entre Amazon S3 y sus instancias. Además de los ejemplos que se explican más abajo, existen muchas herramientas que se han creado para poder obtener acceso a sus datos en Amazon S3 desde su equipo o su instancia. Algunas de las más comunes se explican en los foros de AWS.

Si tiene permiso, puede copiar un archivo entre Amazon S3 y su instancia utilizando uno de los métodos siguientes.

GET or wget (Linux)

> **Note**
>
> Este método solo funciona para objetos públicos. Si el objeto no es público, recibirá un mensaje `ERROR 403: Forbidden`. Si recibe este error, debe utilizar la consola de Amazon S3, la AWS CLI, la API de AWS, los AWS SDK o AWS Tools for Windows PowerShell, y debe disponer de los permisos necesarios. Para obtener más información, consulte Administración de la identidad y el acceso en Amazon S3 y Descarga de un objeto en la Guía del usuario de Amazon S3.

La utilidad wget es un cliente HTTP y FTP que le permite descargar objetos públicos desde Amazon S3. Se instala de forma predeterminada en Amazon Linux y la mayoría de las distribuciones y se puede descargar en Windows. Para descargar un objeto de Amazon S3, utilice el siguiente comando, sustituyendo la URL del objeto que va a descargar.

```
[ec2-user ~]$ wget https://my_bucket.s3.amazonaws.com/path-to-file
```

AWS Tools for Windows PowerShell (Windows)

Las instancias de Windows tienen el beneficio de un navegador gráfico que puede utilizar para obtener acceso a la consola de Amazon S3 directamente. Sin embargo, para los fines

del scripting, los usuarios de Windows también pueden utilizar las AWS Tools for Windows PowerShell para mover objetos desde y hacia Amazon S3.

Utilice el siguiente comando para copiar un objeto de Amazon S3 a su instancia de Windows.

```
PS C:\> Copy-S3Object -BucketName my_bucket -Key path-to-file -
LocalFile my_copied_file.ext
```

AWS CLI (Linux and Windows)

La AWS Command Line Interface (AWS CLI) es una herramienta unificada para administrar los servicios de AWS. La AWS CLI permite a los usuarios autenticarse y descargar elementos restringidos de Simple Storage Service (Amazon S3), además de cargar elementos. Para obtener más información sobre cómo instalar y configurar las herramientas, consulte la página de detalles de AWS Command Line Interface.

El comando aws s3 cp es similar al comando cp de Unix. Puede copiar archivos de Amazon S3 en su instancia, copiar archivos de su instancia en Amazon S3 y copiar archivos de una ubicación de Amazon S3 en otra.

Utilice el siguiente comando para copiar un objeto de Amazon S3 a su instancia.

```
aws s3 cp s3://my_bucket/my_folder/my_file.ext my_copied_file.ext
```

Utilice el siguiente comando para copiar un objeto de su instancia de nuevo en Amazon S3.

```
aws s3 cp my_copied_file.ext s3://my_bucket/my_folder/my_file.ext
```

El comando aws s3 sync puede sincronizar un bucket de Amazon S3 completo en una ubicación de un directorio local. Esto puede facilitar la descarga de un conjunto de datos y mantener la copia local actualizada con el conjunto remoto. Si posee los permisos adecuados en el bucket de Amazon S3, puede enviar su directorio local a la nube cuando haya terminado invirtiendo las ubicaciones de origen y destino en el comando.

Utilice el comando siguiente para descargar un bucket de Amazon S3 completo en un directorio local de su instancia.

```
aws s3 sync s3://remote_S3_bucket local_directory
```

Amazon S3 API

Si es desarrollador, puede utilizar una API para obtener acceso a los datos en Amazon S3. Puede utilizar esta API en el desarrollo de la aplicación e integrarla con otras API y SDK. Para obtener más información, consulte Ejemplos de código para Amazon S3 con SDK de AWS en la Guía del usuario de Amazon S3.

Uso de Amazon EFS con instancias de Linux

> **Note**
>
> No se admite Amazon EFS en las instancias de Windows.

Amazon EFS proporciona almacenamiento de archivos escalable para su uso con Amazon EC2. Puede usar un sistema de archivos de EFS como un origen de datos común para aplicaciones y cargas de trabajo que se ejecutan en varias instancias. Para obtener más información, consulte la página del producto de Amazon Elastic File System.

En este tutorial, se muestra cómo crear y adjuntar un sistema de archivos de Amazon EFS con el asistente de creación rápida de Amazon EFS durante la inicialización de la instancia. Para obtener un tutorial sobre cómo crear un sistema de archivos por medio de la consola de Amazon EFS, consulte Primeros pasos con Amazon Elastic File System en la Guía del usuario de Amazon Elastic File System.

> **Note**
>
> Cuando se crea un sistema de archivos EFS mediante la característica Creación rápida de EFS, la creación del sistema de archivos se realiza con la siguiente configuración recomendada de servicio:
>
> - Copias de seguridad automáticas habilitadas.
> - Destinos de montaje en cada subred predeterminada de la VPC seleccionada.
> - Modo de rendimiento de uso general.
> - Modo de rendimiento por ráfagas.
> - Cifrado de datos en reposo habilitado con la clave predeterminada para Amazon EFS (`aws/elasticfilesystem`).

- Administración del ciclo de vida de Amazon EFS habilitado con una política de 30 días.

Tareas

- Crear un sistema de archivos EFS mediante Creación rápida de Amazon EFS
- Pruebe el sistema de archivos de EFS.
- Elimine el sistema de archivos de EFS.

Crear un sistema de archivos EFS mediante Creación rápida de Amazon EFS

Puede crear un sistema de archivos EFS y montarlo en la instancia en el momento de la inicialización de la misma con la característica Creación rápida de Amazon EFS del asistente de inicialización de instancias en Amazon EC2.

Para crear un sistema de archivos EFS mediante Creación rápida de Amazon EFS,

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. Seleccione Iniciar instancia.
3. (Opcional) En Nombre y etiquetas, escriba un nombre para identificar la instancia en Nombre.
4. En Imágenes de aplicaciones y sistema operativo (Imagen de máquina de Amazon), elija un sistema operativo Linux y, a continuación, para Imagen de máquina de Amazon (AMI), seleccione una AMI de Linux.
5. En Tipo de instancia, para Tipo de instancia, seleccione un tipo de instancia o mantenga el predeterminado.
6. (Opcional) En Par de claves (inicio), para Nombre de par de claves seleccione un par de claves existente o cree uno nuevo.
7. En Configuración de red, elija Editar (a la derecha) y, luego, para Subred, seleccione una subred.

   > **Note**
   >
   > Debe seleccionar una subred antes de poder agregar un sistema de archivos de EFS.

8. En Configurar almacenamiento, elija Editar (en la parte inferior derecha) y, a continuación, haga lo siguiente:

a. En Sistemas de archivos, asegúrese de que EFS esté seleccionado y, a continuación, elija Crear nuevo sistema de archivos compartidos.

b. En Nombre del sistema de archivos, ingrese un nombre para el sistema de archivos de Amazon EFS y, a continuación, seleccione Crear sistema de archivos.

c. En Punto de montaje, especifique un punto de montaje personalizado o mantenga el predeterminado.

d. Para habilitar el acceso al sistema de archivos, seleccione Crear y adjuntar grupos de seguridad de forma automática. Cuando seleccione esta casilla de verificación, los siguientes grupos de seguridad se crearán de forma automática y se adjuntarán a la instancia y a los destinos de montaje del sistema de archivos:

   - Grupo de seguridad de instancia: incluye una regla de salida que permite el tráfico a través del puerto NFS 2049, pero no incluye reglas de entrada.
   - Grupo de seguridad de destinos de montaje del sistema de archivos: incluye una regla de entrada que permite el tráfico a través del puerto NFS 2049 desde el grupo de seguridad de instancias (descrito anteriormente) y una regla de salida que permite el tráfico a través del puerto NFS 2049.

   > **Note**
   >
   > Como alternativa, puede crear y adjuntar los grupos de seguridad de forma manual. Si desea crear y adjuntar los grupos de seguridad de forma manual, desmarque la opción Crear y adjuntar de forma automática los grupos de seguridad necesarios.

e. Para montar de forma automática el sistema de archivos compartidos cuando se lance la instancia, seleccione Montar de forma automática el sistema de archivos compartidos adjuntando el script de datos de usuario necesario. Para ver los datos de usuario que se generan de forma automática, amplíe Detalles avanzados y desplácese hacia abajo hasta Datos de usuario.

   > **Note**
   >
   > Si agregó datos de usuario antes de seleccionar esta casilla de verificación, los datos de usuario originales se sobrescriben con los datos de usuario que se generan de forma automática.

9. Establezca cualquier otra configuración de las instancias como considere necesario.
10. En el panel Resumen, revise la configuración de la instancia y, a continuación, elija Iniciar instancia. Para obtener más información, consulte Lance una instancia con el nuevo asistente de inicialización de instancias.

Pruebe el sistema de archivos de EFS.

Puede conectarse a su instancia y verificar que el sistema de archivos esté montado en el directorio que especificó (por ejemplo, /mnt/efs).

Para verificar que el sistema de archivos esté montado

1. Conecte con la instancia . Para obtener más información, consulte Conexión con la instancia de Linux.
2. De la ventana de terminal de cada instancia, ejecute el comando df -T para verificar que el sistema de archivos EFS esté montado.

```
$ df -T
Filesystem     Type              1K-blocks    Used          Available Use% Mounted
 on
/dev/xvda1     ext4                8123812 1949800            6073764  25% /
devtmpfs       devtmpfs            4078468      56            4078412   1% /dev
tmpfs          tmpfs               4089312       0            4089312   0% /dev/shm
efs-dns        nfs4       9007199254740992       0   9007199254740992   0% /mnt/efs
```

Tenga en cuenta que el nombre del sistema de archivos, que se muestra en el ejemplo como *efs-dns*, tiene la siguiente forma.

```
file-system-id.efs.aws-region.amazonaws.com:/
```

3. (Opcional) Cree un archivo en el sistema de archivos de la instancia y, luego, verifique que pueda ver el archivo desde la otra instancia.

   a. Desde la instancia, ejecute el siguiente comando para crear el archivo.

   ```
   $ sudo touch /mnt/efs/test-file.txt
   ```

   b. Desde la otra instancia, ejecute los siguientes comandos para ver el archivo.

```
$ ls /mnt/efs
test-file.txt
```

Elimine el sistema de archivos de EFS.

Si ya no necesita su sistema de archivos, puede eliminarlo.

Para eliminar el sistema de archivos

1. Abra la consola de Amazon Elastic File System en https://console.aws.amazon.com/efs/.
2. Seleccione el sistema de archivos que va a eliminar.
3. Elija Acciones, Eliminar sistema de archivos.
4. Cuando se le pida confirmación, introduzca el ID del sistema de archivos y elija Eliminar sistema de archivos.

Uso de Amazon FSx con Amazon EC2

La familia de servicios de Amazon FSx facilita la inicialización, la ejecución y el escalado del almacenamiento compartido con tecnología de los sistemas de archivos comerciales y de código abierto populares. Puede utilizar el nuevo asistente de inicialización de instancias para adjuntar de forma automática los siguientes tipos de sistemas de archivos de Amazon FSx a sus instancias de Amazon EC2 durante la inicialización:

- Amazon FSx for NetApp ONTAP proporciona almacenamiento compartido y completamente administrado en la nube de AWS con las populares capacidades de administración y acceso a datos de NetApp ONTAP.
- Amazon FSx for OpenZFS proporciona almacenamiento compartido rentable y completamente administrado con la tecnología del popular sistema de archivos OpenZFS.

> **Note**
>
> - Esta funcionalidad solo está disponible en el nuevo asistente de inicialización de instancias. Para obtener más información, consulte Lance una instancia con el nuevo asistente de inicialización de instancias.

- Los sistemas de archivos de Amazon FSx para Windows File Server y Amazon FSx para Lustre no pueden montarse en la inicialización. Debe montar estos sistemas de archivos de forma manual después de la inicialización.

Puede elegir montar un sistema de archivos existente creado anteriormente o puede crear un nuevo sistema de archivos para montarlo en una instancia durante la inicialización.

Temas

Script de datos de usuario y grupos de seguridad

Cuando monta un sistema de archivos de Amazon FSx en una instancia con el asistente de inicialización de instancias, puede elegir si desea crear y adjuntar de forma automática los grupos de seguridad necesarios para habilitar el acceso al sistema de archivos y si desea incluir de forma automática los scripts de datos de usuario necesarios para montar el sistema de archivos y hacer que esté disponible.

Temas

Grupos de seguridad

Si elige crear de forma automática los grupos de seguridad necesarios para habilitar el acceso al sistema de archivos, el asistente de inicialización de instancias crea y adjunta dos grupos de seguridad: un grupo de seguridad se adjunta a la instancia y el otro se adjunta al sistema de archivos. Para obtener más información sobre los requisitos del grupo de seguridad, consulte el Control de acceso al sistema de archivos de FSx for ONTAP con Amazon VPC y el Control de acceso al sistema de archivos de FSx for OpenZFS con Amazon VPC.

Agregamos la etiqueta `Name=instance-sg-`*1* al grupo de seguridad que se crea y se adjunta a la instancia. El valor de la etiqueta se incrementa de forma automática cada vez que el asistente de inicialización de instancias crea un nuevo grupo de seguridad para los sistemas de archivos de Amazon FSx.

El grupo de seguridad incluye las siguientes reglas de salida, pero no reglas de entrada.

Reglas de salida

Tipo de protocolo	Número de puerto	Destino
UDP	111	*grupo de seguridad del sistema de archivos*
UDP	20001 - 20003	*grupo de seguridad del sistema de archivos*
UDP	4049	*grupo de seguridad del sistema de archivos*
UDP	2049	*grupo de seguridad del sistema de archivos*
UDP	635	*grupo de seguridad del sistema de archivos*
UDP	4045 - 4046	*grupo de seguridad del sistema de archivos*
TCP	4049	*grupo de seguridad del sistema de archivos*
TCP	635	*grupo de seguridad del sistema de archivos*
TCP	2049	*grupo de seguridad del sistema de archivos*
TCP	111	*grupo de seguridad del sistema de archivos*
TCP	4045 - 4046	*grupo de seguridad del sistema de archivos*

Tipo de protocolo	Número de puerto	Destino
TCP	20001 - 20003	*grupo de seguridad del sistema de archivos*
Todos	Todos	*grupo de seguridad del sistema de archivos*

El grupo de seguridad que se crea y se adjunta al sistema de archivos se etiqueta con `Name=fsx-sg-`*1*. El valor de la etiqueta se incrementa de forma automática cada vez que el asistente de inicialización de instancias crea un nuevo grupo de seguridad para los sistemas de archivos de Amazon FSx.

El grupo de seguridad incluye las siguientes reglas.

Reglas de entrada

Tipo de protocolo	Número de puerto	Origen
UDP	2049	*grupo de seguridad de instancia*
UDP	20001 - 20003	*grupo de seguridad de instancia*
UDP	4049	*grupo de seguridad de instancia*
UDP	111	*grupo de seguridad de instancia*
UDP	635	*grupo de seguridad de instancia*
UDP	4045 - 4046	*grupo de seguridad de instancia*
TCP	4045 - 4046	*grupo de seguridad de instancia*
TCP	635	*grupo de seguridad de instancia*
TCP	2049	*grupo de seguridad de instancia*
TCP	4049	*grupo de seguridad de instancia*
TCP	20001 - 20003	*grupo de seguridad de instancia*

Tipo de protocolo	Número de puerto	Origen
TCP	111	*grupo de seguridad de instancia*

Reglas de salida

Tipo de protocolo	Número de puerto	Destino
Todos	Todos	0.0.0.0/0

Script de datos de usuario

Si elige adjuntar de forma automática los scripts de datos de usuario, el asistente de inicialización de instancias agrega los siguientes datos de usuario a la instancia. Este script instala los paquetes necesarios, monta el sistema de archivos y actualiza la configuración de la instancia para que el sistema de archivos se vuelva a montar de forma automática cada vez que se reinicie la instancia.

```
#cloud-config
package_update: true
package_upgrade: true
runcmd:
- yum install -y nfs-utils
- apt-get -y install nfs-common
- svm_id_1=svm_id
- file_system_id_1=file_system_id
- vol_path_1=/vol1
- fsx_mount_point_1=/mnt/fsx/fs1
- mkdir -p "${fsx_mount_point_1}"
- if [ -z "$svm_id_1" ]; then printf "\n${file_system_id_1}.fsx.eu-
north-1.amazonaws.com:/${vol_path_1} ${fsx_mount_point_1} nfs4
 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport,_netdev
 0 0\n" >> /etc/fstab; else printf "\n${svm_id_1}.${file_system_id_1}.fsx.eu-
north-1.amazonaws.com:/${vol_path_1} ${fsx_mount_point_1} nfs4
 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport,_netdev 0
 0\n" >> /etc/fstab; fi
- retryCnt=15; waitTime=30; while true; do mount -a -t nfs4 defaults; if [ $? = 0 ] ||
 [ $retryCnt -lt 1 ]; then echo File system mounted successfully; break; fi; echo File
 system not available, retrying to mount.; ((retryCnt--)); sleep $waitTime; done;
```

Montaje de un sistema de archivos de Amazon FSx en la inicialización

Para montar un sistema de archivos de Amazon FSx nuevo o existente en la inicialización

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instancias y luego elija Iniciar instancia para abrir el asistente de inicialización de instancias.
3. En la sección Application and OS Images (Imágenes de aplicaciones y sistema operativo), seleccione la AMI que desea utilizar.
4. En la sección Tipo de instancia, seleccione el tipo de instancia.
5. En la sección Par de claves, seleccione un par de claves existente o cree uno nuevo.
6. En la sección Configuración de red, realice lo siguiente:
   a. Elija Editar.
   b. Si desea montar un sistema de archivos de existente, en Subred, elija la subred preferida del sistema de archivos. Se recomienda iniciar la instancia en la misma zona de disponibilidad que la subred preferida del sistema de archivos para optimizar el rendimiento.

      Si desea crear un sistema de archivos nuevo para montarlo en una instancia, en Subred, elija la subred en la que desea iniciar la instancia.

      > **Important**
      >
      > Debe seleccionar una subred para habilitar la funcionalidad de Amazon FSx en el nuevo asistente de inicialización de instancias. Si no selecciona una subred, no podrá montar un sistema de archivos existente ni crear uno nuevo.

7. En la sección Almacenamiento, haga lo siguiente:
   a. Configure los volúmenes según sea necesario.
   b. Expanda la sección Sistemas de archivos y seleccione FSx.
   c. Elija Agregar sistema de archivos compartidos.
   d. En Sistemas de archivos, seleccione el sistema de archivos que desea montar.

> **Note**
>
> En la lista se muestran todos los sistemas de archivos de Amazon FSx for NetApp ONTAP y Amazon FSx for OpenZFS en la cuenta de la región seleccionada.

e. Para crear y adjuntar de forma automática los grupos de seguridad necesarios para habilitar el acceso al sistema de archivos, seleccione Crear y adjuntar grupos de seguridad de forma automática. Si prefiere crear los grupos de seguridad de forma manual, desactive la casilla de verificación. Para obtener más información, consulte Grupos de seguridad.

f. Para adjuntar de forma automática los scripts de datos de usuario necesarios para montar el sistema de archivos, seleccione Automatically mount shared file system by attaching required user data script (Montar de forma automática el sistema de archivos compartidos adjuntando el script de datos de usuario necesario). Si prefiere proporcionar los scripts de datos de usuario de forma manual, desactive la casilla de verificación. Para obtener más información, consulte Script de datos de usuario.

8. En la sección Opciones avanzadas, establezca las configuraciones adicionales de la instancia según sea necesario.
9. Elija Iniciar.

Uso de Amazon File Cache con Amazon EC2

Amazon File Cache es una memoria caché de alta velocidad totalmente administrada en AWS que se utiliza para procesar datos de archivos, independientemente de dónde estén almacenados los datos. Amazon File Cache sirve como ubicación de almacenamiento temporal de alto rendimiento para los datos que se almacenan en sistemas de archivos en las instalaciones, sistemas de archivos de AWS y buckets de Amazon Simple Storage Service (Amazon S3). Puede utilizar esta capacidad para hacer que los conjuntos de datos dispersos estén disponibles para las aplicaciones basadas en archivos en AWS con una vista unificada y a altas velocidades, con latencias inferiores a un milisegundo y alto rendimiento. Para obtener más información, consulte ¿Qué es Amazon File Cache?

Puede acceder a su caché desde sus instancias de Amazon EC2 mediante el cliente Lustre de código abierto. Las instancias de Amazon EC2 pueden acceder a su caché desde otras zonas de disponibilidad dentro de la misma Amazon Virtual Private Cloud (Amazon VPC), siempre y cuando su red permita el acceso a través de subredes dentro de la VPC. Una vez montada la caché, puede trabajar con los archivos y directorios como haría con cualquier sistema de archivos local.

Para comenzar, consulte Introducción a Amazon File Cache.

Límites de volumen de instancias

La cantidad máxima de volúmenes de Amazon EBS que puede adjuntar a una instancia depende del tipo y tamaño de la instancia. Al determinar cuántos volúmenes adjuntar a la instancia, debe tener en cuenta si necesita un mayor ancho de banda de E/S o una mayor capacidad de almacenamiento.

Ancho de banda frente a capacidad

Para obtener casos de uso de ancho de banda uniformes y predecibles, utilice instancias optimizadas para Amazon EBS con volúmenes de SSD de uso general o volúmenes de SSD de IOPS aprovisionadas. Para un máximo rendimiento, iguale las IOPS que ha aprovisionado para sus volúmenes con el ancho de banda disponible para su tipo de instancia.

En configuraciones RAID, puede notar que las matrices superiores a 8 volúmenes reducen el rendimiento, debido a un aumento del trabajo de E/S. Pruebe el rendimiento de su aplicación individual y ajústelo cuanto sea necesario.

Temas

- Límites de volumen para las instancias basadas en Nitro System
- Límites de volumen para instancias basadas en Xen

Límites de volumen para las instancias basadas en Nitro System

Temas

- Límite de volumen dedicado de Amazon EBS
- Límite de volumen compartido de Amazon EBS

Límite de volumen dedicado de Amazon EBS

Los siguientes tipos de instancias de Nitro tienen un límite de volúmenes dedicados de Amazon EBS que varía según el tamaño de la instancia. El límite no se comparte con los archivos adjuntos de otros dispositivos. En otras palabras, puede adjuntar cualquier cantidad de volúmenes de Amazon EBS hasta el límite de volúmenes adjuntos, independientemente de la cantidad de dispositivos conectados, como los volúmenes del almacén de instancias de NVMe y las interfaces de red.

- De uso general: M7a, M7i, M7i-flex
- Optimizadas para la computación: C7a, C7i
- Optimizadas para memoria: R7a, R7i, R7iz

Para estos tipos de instancias que admiten límites de volumen dedicados, los límites de volumen dependen del tamaño de la instancia. En la siguiente tabla se muestra el límite para cada tamaño de instancia.

Tamaño de instancia	Límite de volumen
`medium | large | xlarge | 2xlarge | 4xlarge | 8xlarge | 12xlarge`	32
`16xlarge`	48
`24xlarge`	64
`32xlarge`	88
`48xlarge`	128
`metal-16xl | metal-24xl`	39
`metal-32xl | metal-48xl`	79

Límite de volumen compartido de Amazon EBS

Todos los demás tipos de instancia de Nitro (que no se muestran en Límite de volumen dedicado de Amazon EBS) tienen un límite de adición de volumen que se comparte entre los volúmenes de Amazon EBS, las interfaces de red y los volúmenes de almacén de instancia de NVMe. Puede adjuntar cualquier cantidad de volúmenes de Amazon EBS hasta ese límite, menos la cantidad de interfaces de red conectadas y los volúmenes del almacén de instancias de NVMe. Tenga en cuenta que cada instancia debe tener al menos una interfaz de red y que los volúmenes del almacén de instancias de NVMe se adjuntan automáticamente en el momento de la inicialización.

La mayoría de estas instancias admite un máximo de 28 adjuntos. Por ejemplo, si no tiene más elementos de interfaz de red asociados en una instancia `m5.xlarge`, le puede asociar un máximo de 27 volúmenes de EBS (límite de volumen de 28 - 1 interfaz de red). Si tiene dos interfaces de red adicionales en una instancia `m5.xlarge`, puede adjuntar hasta 25 volúmenes de EBS (límite de volumen de 28 - 3 interfaces de red). Del mismo modo, si tiene dos interfaces de red adicionales en una instancia `m5d.xlarge`, que tiene 1 volumen de almacén de instancias de NVMe, puede adjuntar hasta 24 volúmenes de EBS (límite de volumen de 28 - 3 interfaces de red - 1 volumen de almacén de instancias NVMe).

Las siguientes excepciones para los tipos de instancias que tienen límites de volumen compartidos:

- Las instancias DL2q admiten un máximo de 19 volúmenes de EBS.
- La mayoría de las instancias bare metal admiten un máximo de 31 volúmenes de EBS.
- Las instancias virtualizadas de memoria elevada admiten un máximo de 27 volúmenes de EBS.
- Las instancias bare metal de memoria elevada admiten un máximo de 19 volúmenes de EBS.
- Las instancias `inf1.xlarge` y `inf1.2xlarge` admiten un máximo de 26 volúmenes de EBS.
- Las instancias `inf1.6xlarge` admiten un máximo de 23 volúmenes de EBS.
- Las instancias `mac1.metal` admiten un máximo de 16 volúmenes de EBS.
- Las instancias `mac2.metal`, `mac2-m2.metal` y `mac2-m2pro.metal` admiten un máximo de 10 volúmenes de EBS.
- Las instancias `inf1.24xlarge` admiten un máximo de 11 volúmenes de EBS.
- Las instancias `g5.48xlarge` admiten un máximo de 9 volúmenes de EBS.
- Las instancias `d3.8xlarge` y `d3en.12xlarge` admiten un máximo de 3 volúmenes de EBS.
- Para las instancias de computación acelerada, los aceleradores adjuntos cuentan para el límite de volumen compartido. Por ejemplo, para las instancias `p4d.24xlarge`, que tienen un límite de volumen compartido de 28, 8 GPU y 8 volúmenes de almacén de instancias de NVMe, puede adjuntar hasta 11 volúmenes de Amazon EBS (límite de volumen de 28 - 1 interfaz de red - 8 GPU - 8 volúmenes de almacén de instancias NVMe).

Límites de volumen para instancias basadas en Xen

instancias de Linux

Adjuntar más de 40 volúmenes a una instancia de Linux basada en Xen puede provocar errores de arranque. Tenga en cuenta que esta cantidad incluye el volumen raíz, además de cualquier volumen de almacén de instancias asociado y los volúmenes de Amazon EBS.

Si tiene problemas de arranque en una instancia con un gran número de volúmenes, detenga la instancia, quite los volúmenes que no sean esenciales para el proceso de arranque, arranque la instancia y vuelva a adjuntar los volúmenes después de que la instancia se esté ejecutando.

> **Important**
>
> Adjuntar más de 40 volúmenes a una instancia de Linux basada en Xen solo se admite como medida excepcional y no se garantiza.

instancias de Windows

La siguiente tabla muestra los límites de volumen de las instancias de Windows basadas en Xen según el controlador utilizado. Tenga en cuenta que estas cantidades incluyen el volumen raíz, además de cualquier volumen de almacén de instancias adjunto y los volúmenes de Amazon EBS.

> **Important**
>
> Adjuntar más de los siguientes volúmenes a una instancia de Windows basada en Xen solo se admite como medida excepcional y no se garantiza.

Controlador	Límite de volumen
AWS PV	26
Citrix PV	26
Red Hat PV	17

Recomendamos que no adjunte a una instancia de Windows basada en Xen más de 26 volúmenes con controladores como PV o Citrix PV de AWS, ya que probablemente se producirán problemas de rendimiento. Para determinar los controladores PV que está utilizando la instancia, o para actualizar la instancia de Windows desde controladores Red Hat a Citrix PV, consulte the section called “Actualizar controladores PV”.

Para obtener más información sobre la relación entre los nombres de los dispositivos y los volúmenes, consulte Asignar discos a volúmenes en instancia de Windows.

Volumen raíz de la instancia de Amazon EC2

Cuando se inicia una instancia, se crea un volumen raíz para dicha instancia. El volumen raíz contiene la imagen que se usa para arrancar dicha instancia. Cada instancia tiene un único volumen raíz. Puede agregar volúmenes de almacenamiento a las instancias durante o después de la inicialización.

Reservamos nombres de dispositivos específicos para los volúmenes raíz. Para obtener más información, consulte Nombres de dispositivos en las instancias de Amazon EC2.

Contenido

Tipo de volumen raíz

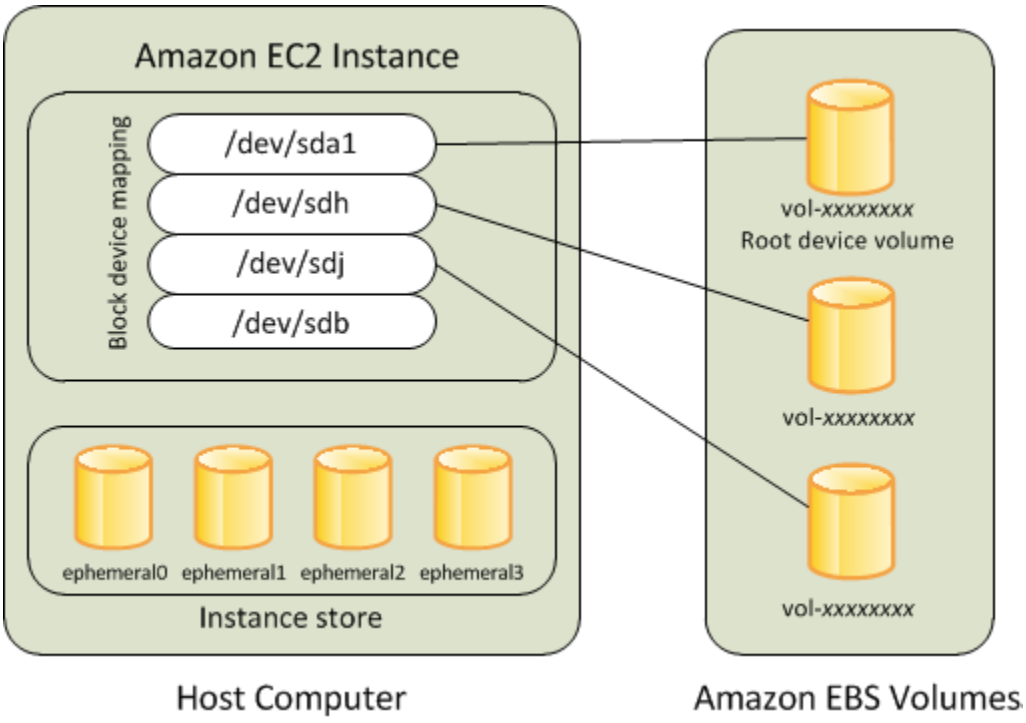
La AMI que usa para iniciar una instancia determina el tipo de volumen raíz. Puede iniciar una instancia desde una AMI basada en Amazon EBS (instancias de Linux y Windows) o bien desde una AMI con respaldo en el almacén de instancias (solo instancias de Linux). Hay diferencias significativas respecto a lo que se puede hacer con cada tipo de AMI. Para obtener más información sobre estas diferencias, consulte Almacenamiento para el dispositivo raíz.

Le recomendamos que utilice AMI respaldadas por Amazon EBS, ya que estas instancias se inician más rápido y utilizan un almacenamiento persistente.

instancias respaldadas por Amazon EBS

Las instancias que utilizan Amazon EBS para el volumen raíz tienen automáticamente un volumen de Amazon EBS asociado. Cuando se inicia una instancia respaldada por Amazon EBS, se crea un volumen de Amazon EBS para cada instantánea de Amazon EBS a la que hace referencia la AMI que se está utilizando. Si lo desea, puede utilizar otros volúmenes de Amazon EBS o volúmenes almacén de instancias, dependiendo del tipo de instancia.

Una instancia respaldada por Amazon EBS se puede parar y reiniciar posteriormente sin que ello afecte a los datos almacenados en los volúmenes adjuntos. Existen distintas tareas relacionadas con la instancia y con el volumen que puede realizar cuando una instancia respaldada por Amazon EBS está en estado detenido. Por ejemplo, puede modificar las propiedades de la instancia, cambiar su tamaño o actualizar el kernel que utiliza, o bien puede asociar el volumen raíz a otra instancia en ejecución para fines de depuración o para cualquier otro fin. Para obtener más información, consulte Volúmenes de Amazon EBS.



Limitación

No puede usar los volúmenes de EBS `st1` o `sc1` como volúmenes raíz.

Error en una instancia

Si una instancia respaldada por Amazon EBS falla, puede restaurar la sesión siguiendo uno de estos métodos:

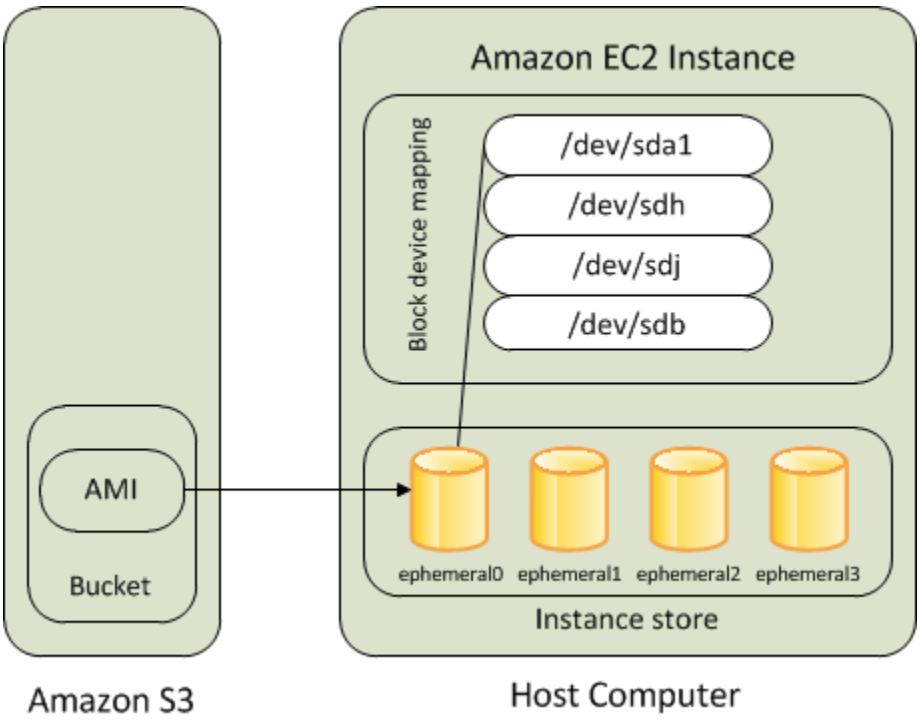
- Detenga la instancia y vuelva a iniciarla (pruebe este método en primer lugar).
- Haga una instantánea automáticamente de todos los volúmenes pertinentes y cree una nueva AMI. Para obtener más información, consulte Creación de una AMI basada en Amazon EBS.
- Adjunte el volumen a la nueva instancia siguiendo estos pasos:
  1. Cree una instantánea del volumen raíz.
  2. Registre una nueva AMI utilizando la instantánea.
  3. Lance una nueva instancia nueva desde la nueva AMI.
  4. Separe los volúmenes de Amazon EBS restantes de la antigua instancia.
  5. Adjunte los volúmenes de Amazon EBS a la instancia nueva.

Instancias con respaldo en el almacén de instancias (solo instancias de Linux)

> **Note**
>
> Las instancias de Windows no admiten volúmenes raíz respaldados por un almacén de instancias.

Las instancias que utilizan el almacén de instancias para el volumen raíz tienen automáticamente uno o varios volúmenes de almacén de instancias disponibles, uno de los cuales funciona como volumen raíz. Cundo se inicia una instancia, la imagen utilizada para arrancar dicha instancia se copia en el volumen raíz. Tenga en cuenta que puede utilizar volúmenes de almacén de instancias adicionales de manera opcional, dependiendo del tipo de instancia.

Los datos de volúmenes de almacén de instancias persisten siempre que la instancia esté en ejecución, pero estos datos se eliminan cuando la instancia se termina (las instancias con respaldo en el almacén de instancias no admiten la acción Detener) o si falla (por ejemplo, si una unidad subyacente tiene problemas). Para obtener más información, consulte Almacén de instancias Amazon EC2.



Requisito

Sólo los siguientes tipos de instancia admiten un volumen de almacén de instancia como volumen raíz: C3, D2, I2, M3 y R3.

Error en una instancia

Cuando una instancia con respaldo en el almacenamiento falla o se termina, no se puede restaurar. Si tiene previsto utilizar instancias Amazon EC2 con respaldo en el almacén de instancias, es muy recomendable que distribuya los datos de los almacenes de instancias entre varias zonas de disponibilidad. También debería hacer un backup de los datos de importancia crítica de los volúmenes de almacén de instancias en un almacenamiento persistente con regularidad.

Elección de una AMI de Linux por tipo de volumen raíz

> **Note**
>
> Todas las AMI de Windows están respaldadas por EBS.

La AMI que se especifica cuando se inicia una instancia determina el tipo de volumen de dispositivo raíz que tiene dicha instancia. Puede ver las AMI por tipo de dispositivo raíz utilizando alguno de los métodos siguientes.

Console

Para elegir una AMI respaldada por Amazon EBS con la consola

1. Abra la consola de Amazon EC2.
2. En el panel de navegación, elija AMIs.
3. En las listas de filtros, seleccione el tipo de imagen (por ejemplo, Imágenes públicas). En la barra de búsqueda, elija Plataforma para seleccionar el sistema operativo (por ejemplo, Amazon Linux) y Tipo de dispositivo raíz para seleccionar el tipo de volumen raíz (ebs o instance-store).
4. (Opcional) Para obtener información adicional que pueda ser de ayuda para su elección, elija el icono Preferencias, cambie las columnas que se muestran y elija Confirmar.
5. Elija una AMI y anote su ID de AMI.

AWS CLI

Para verificar el tipo de volumen de dispositivo raíz de una AMI con la línea de comando

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

- describe-images (AWS CLI)
- Get-EC2Image (AWS Tools for Windows PowerShell)

Determinación del tipo de dispositivo raíz de la instancia de Linux

> **Note**
>
> Las instancias de Windows deben tener el respaldo en EBS.

Puede ver el tipo de dispositivo raíz de la instancia de Linux utilizando alguno de los métodos siguientes.

Console

Para determinar el tipo de dispositivo raíz de una instancia con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instancias y seleccione la instancia.
3. En la pestaña Almacenamiento, en Detalles del dispositivo raíz, compruebe el valor del Tipo de dispositivo raíz del siguiente modo:
   - Si el valor es `EBS`, se trata de una instancia respaldada por Amazon EBS.
   - Si el valor es `INSTANCE-STORE`, se trata de una instancia con respaldo en el almacén de instancias.

AWS CLI

Para determinar el tipo de dispositivo raíz de una instancia con la línea de comando

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

- describe-instances (AWS CLI)
- Get-EC2Instance (AWS Tools for Windows PowerShell)

Cambiar el volumen raíz a para que persista

De forma predeterminada, el volumen raíz de una AMI respaldada por Amazon EBS se elimina cuando se termina la instancia. Puede cambiar el comportamiento predeterminado para asegurarse de que el volumen persiste después de que termine la instancia. Para cambiar el comportamiento predeterminado, establezca el atributo `DeleteOnTermination` como `false` mediante una asignación de dispositivos de bloques.

Tareas

- Configurar el volumen raíz para que persista durante el lanzamiento de la instancia
- Configurar el volumen raíz para que persista en una instancia existente
- Confirmar que un volumen raíz está configurado para persistir

Configurar el volumen raíz para que persista durante el lanzamiento de la instancia

Puede configurar el volumen raíz para que persista al iniciar una instancia mediante la consola de Amazon EC2 o las herramientas de línea de comandos.

Console

Para configurar el volumen raíz para que persista al iniciar una instancia mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instancias y elija Iniciar instancias.
3. Elija una imagen de máquina de Amazon (AMI), elija un tipo de instancia, elija un par de claves y configure los ajustes de red.
4. En Configurar almacenamiento, seleccione Avanzado.
5. Amplíe el volumen raíz.
6. En Eliminar al terminar, elija No.
7. Cuando termine de configurar la instancia, elija Iniciar instancia.

AWS CLI

Para configurar el volumen raíz para que persista al iniciar una instancia mediante la AWS CLI

Utilice el comando run-instances e incluya una asignación de dispositivos de bloque que establezca el atributo `DeleteOnTermination` en `false`.

```
aws ec2 run-instances --block-device-mappings file://mapping.json ...other
 parameters...
```

En `mapping.json`, especifique lo siguiente.

```
[
    {
        "DeviceName": "/dev/sda1",
        "Ebs": {
            "DeleteOnTermination": false
        }
    }
]
```

Tools for Windows PowerShell

Para configurar el volumen raíz para que persista al iniciar una instancia mediante Tools for Windows PowerShell

Utilice el comando New-EC2Instance e incluya una asignación de dispositivos de bloque que establezca el atributo `DeleteOnTermination` en `false`.

```
C:\> $ebs = New-Object Amazon.EC2.Model.EbsBlockDevice
C:\> $ebs.DeleteOnTermination = $false
C:\> $bdm = New-Object Amazon.EC2.Model.BlockDeviceMapping
C:\> $bdm.DeviceName = "dev/xvda"
C:\> $bdm.Ebs = $ebs
C:\> New-EC2Instance -ImageId ami-0abcdef1234567890 -BlockDeviceMapping
 $bdm ...other parameters...
```

Configurar el volumen raíz para que persista en una instancia existente

Puede configurar el volumen raíz para que persista en una instancia en ejecución utilizando únicamente las herramientas de línea de comandos.

AWS CLI

Para configurar el volumen raíz para que persista en una instancia existente mediante AWS CLI

Utilice el comando modify-instance-attribute con una asignación de dispositivo de bloque que establezca el atributo `DeleteOnTermination` en `false`.

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --block-device-
mappings file://mapping.json
```

En `mapping.json`, especifique lo siguiente.

```
[
    {
        "DeviceName": "/dev/xvda",
        "Ebs": {
            "DeleteOnTermination": false
        }
    }
```

```
]
```

Tools for Windows PowerShell

Para configurar el volumen raíz para que persista en una instancia existente mediante AWS Tools for Windows PowerShell

Utilice el comando Edit-EC2InstanceAttribute con una asignación de dispositivo de bloque que establezca el atributo `DeleteOnTermination` en `false`.

```
C:\> $ebs = New-Object Amazon.EC2.Model.EbsInstanceBlockDeviceSpecification
C:\> $ebs.DeleteOnTermination = $false
C:\> $bdm = New-Object Amazon.EC2.Model.InstanceBlockDeviceMappingSpecification
C:\> $bdm.DeviceName = "/dev/xvda"
C:\> $bdm.Ebs = $ebs
C:\> Edit-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -BlockDeviceMapping
 $bdm
```

Confirmar que un volumen raíz está configurado para persistir

Puede confirmar que un volumen raíz está configurado para que persista utilizando la consola de Amazon EC2 o las herramientas de línea de comandos.

Console

Para confirmar que un volumen raíz está configurado para que persista utilizando la consola de Amazon EC2

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instancias y, a continuación, seleccione la instancia.
3. En la pestaña Almacenamiento, en Dispositivos de bloques, localice la entrada para el volumen raíz. Si Eliminar al terminar es No, el volumen está configurado para persistir.

AWS CLI

Para confirmar que un volumen raíz está configurado para que persista utilizando la AWS CLI

Utilice el comando describe-instances y compruebe que el atributo `DeleteOnTermination` del elemento de respuesta `BlockDeviceMappings` esté establecido en `false`.

```
aws ec2 describe-instances --instance-id i-1234567890abcdef0
```

```
...
    "BlockDeviceMappings": [
    {
        "DeviceName": "/dev/sda1",
        "Ebs": {
            "Status": "attached",
            "DeleteOnTermination": false,
            "VolumeId": "vol-1234567890abcdef0",
            "AttachTime": "2013-07-19T02:42:39.000Z"
        }
    }
...
```

Tools for Windows PowerShell

Para confirmar que un volumen raíz está configurado para que persista utilizando la AWS Tools for Windows PowerShell

Utilice Get-EC2Instance y compruebe que el atributo `DeleteOnTermination` del elemento de respuesta `BlockDeviceMappings` está establecido en `false`.

```
C:\> (Get-EC2Instance -InstanceId i-
i-1234567890abcdef0).Instances.BlockDeviceMappings.Ebs
```

Cambiar el tamaño inicial del volumen raíz

De forma predeterminada, el tamaño del volumen raíz viene determinado por el tamaño de la instantánea. Puede aumentar el tamaño inicial del volumen raíz mediante la asignación de dispositivos de bloque de la instancia de la siguiente manera.

1. Determine el nombre del dispositivo del volumen raíz especificado en la AMI, como se describe en Visualizar los volúmenes de EBS en una asignación de dispositivos de bloques de una AMI.
2. Confirme el tamaño de la instantánea indicada en la asignación de dispositivos de bloques de AMI.
3. Sustituya el tamaño del volumen raíz mediante la asignación de dispositivos de bloque de instancia, como se describe en Actualizar la asignación de dispositivos de bloques al iniciar una instancia y especifique un tamaño de volumen mayor que el tamaño de la instantánea.

Por ejemplo, la siguiente entrada para la asignación de dispositivos de bloque de instancia aumenta el tamaño del volumen raíz, `/dev/xvda`, a 100 GiB. Puede omitir el ID de instantánea en la asignación de dispositivo de bloque de instancia porque el ID de instantánea ya está especificado en la asignación de dispositivos de bloque AMI.

```
{
    "DeviceName": "/dev/xvda",
    "Ebs": {
      "VolumeSize": 100
    }
}
```

Para obtener más información, consulte Mapeos de dispositivos de bloques.

Sustitución de un volumen raíz de la instancia de EC2

Amazon EC2 permite reemplazar el volumen raíz de Amazon EBS para una instancia en ejecución a la vez que se retiene lo siguiente:

- Datos almacenados en volúmenes de almacén de instancias: los volúmenes de almacén de instancias permanecen asociados a la instancia después de reemplazar el volumen raíz.
- Datos almacenados en volúmenes de Amazon EBS de datos (que no son raíz): los volúmenes de Amazon EBS que no son raíz permanecen asociados a la instancia después de restaurar el volumen raíz.
- Configuración de red: todas las interfaces de red permanecen asociadas a la instancia y conservan sus direcciones IP, identificadores e ID de datos asociados. Cuando la instancia está disponible, se vacía todo el tráfico de red pendiente. Además, la instancia permanece en el mismo host físico, por lo que conserva sus direcciones IP públicas y privadas y su nombre DNS.
- Políticas de IAM: se conservan y se aplican los perfiles y las políticas de IAM (como las políticas basadas en etiquetas) que están asociados a la instancia.

Temas

- ¿Cómo funciona?
- Reemplazar un volumen raíz
- Ver tareas de reemplazo de volumen raíz

¿Cómo funciona?

Cuando reemplaza el volumen raíz de una instancia, un volumen raíz nuevo (de reemplazo) se restaura de una de las maneras siguientes:

- Al estado de inicialización inicial: el volumen se restaura al estado inicial en la inicialización de la instancia. Para obtener más información, consulte Restaurar un volumen raíz a su estado de inicialización.
- A partir de una instantánea del mismo linaje que el volumen raíz actual: esto permite corregir problemas, como daños en el volumen raíz o errores de configuración de red del sistema operativo invitado. Para obtener más información, consulte Reemplazar un volumen raíz mediante una instantánea.
- A partir de una AMI que tenga los mismos atributos clave que la instancia: esto le permite hacer actualizaciones o aplicar revisiones del sistema operativo y de las aplicaciones. Para obtener más información, consulte Reemplazar un volumen raíz mediante una AMI.

El volumen raíz original se separa de la instancia y el volumen raíz nuevo se adjunta a la instancia en su lugar. La asignación de dispositivos de bloques de la instancia se actualiza para reflejar el ID del volumen raíz de reemplazo. Puede elegir si desea conservar o no el volumen raíz original una vez finalizado su proceso de reemplazo. Si decide eliminar el volumen raíz original cuando haya finalizado el proceso de reemplazo, se eliminará automáticamente y ya no se podrá recuperar. Si decide conservar el volumen raíz original cuando haya finalizado el proceso, permanecerá aprovisionado en su cuenta y deberá eliminarlo manualmente cuando ya no lo necesite.

Si la tarea de reemplazo del volumen raíz tiene errores, la instancia se reiniciará y el volumen raíz original permanecerá adjunto a ella.

Consideraciones para reemplazar el volumen raíz

- La instancia debe tener el estado `running`.
- La instancia se reinicia automáticamente durante el proceso. El contenido de la memoria (RAM) se borra durante el reinicio. No se requieren reinicios manuales.
- No puede reemplazar el volumen raíz si se trata de un volumen de almacén de instancias. Solo se admiten las instancias con volúmenes raíz de Amazon EBS.
- Puede reemplazar el volumen raíz de todos los tipos de instancia virtualizados y las instancias bare metal de EC2 Mac. No se admite ninguna otra instancia bare metal.

- Puede utilizar cualquier instantánea que pertenezca al mismo linaje que cualquiera de los volúmenes raíz anteriores de la instancia.
- Si la cuenta está habilitada para cifrado de Amazon EBS de forma predeterminada en la región actual, el volumen raíz de reemplazo creado por la tarea de reemplazo del volumen raíz siempre está cifrado, independientemente del estado de cifrado de la instantánea especificada o del volumen raíz de la AMI especificada.
- En la tabla siguiente, se resumen los posibles resultados de cifrado.

	Volumen raíz original	Instantánea o AMI especificadas	Cifrado de forma predeterminada	Volumen raíz de reemplazo	Clave de cifrado utilizada para reemplazar el volumen raíz
Restaurar el volumen raíz de reemplazo al estado de inicialización inicial	Encriptado	No aplicable	No se considera	Encriptado	Misma clave de KMS que el volumen raíz original
	Sin cifrar	No aplicable	Deshabilitad	Sin cifrar	No aplicable
	Sin cifrar	No aplicable	Habilitado	Encriptado	Clave de KMS predeterminada para el cifrado de Amazon EBS de la cuenta
Restaurar el volumen raíz de reemplazo desde una	Encriptado	Sin cifrar	No se considera	Encriptado	Misma clave de KMS que el volumen raíz original

	Volumen raíz original	Instantánea o AMI especificadas	Cifrado de forma predeterminada	Volumen raíz de reemplazo	Clave de cifrado utilizada para reemplazar el volumen raíz
instantánea o una AMI	Encriptado	Encriptado	No se considera	Encriptado	Misma clave de KMS que el volumen raíz original
	Sin cifrar	Sin cifrar	Deshabilitad	Sin cifrar	No aplicable
	Sin cifrar	Sin cifrar	Habilitado	Encriptado	Clave de KMS predeterminada para el cifrado de Amazon EBS de la cuenta

	Volumen raíz original	Instantánea o AMI especificadas	Cifrado de forma predeterminada	Volumen raíz de reemplazo	Clave de cifrado utilizada para reemplazar el volumen raíz
	Sin cifrar	Encriptado	No se considera	Encriptado	Si la AMI o la instantánea son propiedad de la cuenta, el volumen de reemplazo se cifra con la clave de KMS de la AMI o la instantánea. Si la AMI o la instantánea se comparten con la cuenta, el volumen de reemplazo se cifra con la clave de KMS predeterminada para el cifrado de Amazon EBS de la cuenta.

Temas

Restaurar un volumen raíz a su estado de inicialización

Puede reemplazar el volumen raíz de una instancia por otro que se restablezca a su estado de inicialización original. El volumen de reemplazo se restaura automáticamente a partir de la instantánea utilizada para crear el volumen original durante la inicialización de la instancia.

El volumen raíz de reemplazo tendrá los mismos atributos que el original: tipo, tamaño y eliminación al terminar la instancia.

Reemplazar un volumen raíz mediante una instantánea

Puede reemplazar el volumen raíz de una instancia por otro que se restablezca a una instantánea específica. Esto permite restaurar el volumen raíz de una instancia a una instantánea específica creada anteriormente mediante ese volumen raíz.

El volumen raíz de reemplazo tendrá los mismos atributos que el original: tipo, tamaño y eliminación al terminar la instancia.

Consideraciones para utilizar una instantánea

- Solo se pueden utilizar instantáneas que pertenezcan al mismo linaje que el volumen raíz actual de la instancia.
- No puede usar copias de instantáneas creadas a partir de instantáneas tomadas del volumen raíz.
- Después de restaurar correctamente el volumen raíz, las instantáneas tomadas desde el volumen raíz original aún se podrán utilizar para reemplazar el nuevo volumen raíz (de reemplazo).

Reemplazar un volumen raíz mediante una AMI

Puede reemplazar el volumen raíz mediante una AMI de su propiedad o una AMI compartida con usted. La AMI debe tener el mismo código de producto, información de facturación, tipo de arquitectura y tipo de virtualización que los de la instancia.

Si la instancia está habilitada para NitroTPM, ENA o sriov-net, debe usar una AMI que admita esas características. Si la instancia no está habilitada para ENA o sriov-net, puede seleccionar una AMI

que no admita esas características o puede añadir soporte automáticamente si selecciona una AMI que admita ENA o sriov-net.

Si la instancia está habilitada para NitroTPM, debe usar una AMI que tenga NitroTPM habilitado. La compatibilidad con NitroTPM no está habilitada si la instancia no se configuró para ello, independientemente de la AMI que seleccione.

Puede seleccionar una AMI con un modo de arranque diferente al de la instancia, siempre que esta lo admita. Si la instancia no admite el modo de arranque, se produce un error en la solicitud. Si la instancia admite el modo de arranque, este se propaga a la instancia y sus datos de UEFI se actualizan en consecuencia. Si modificó manualmente el orden de arranque o agregó una clave privada de arranque seguro UEFI para cargar los módulos del kernel privado, los cambios se perderán al reemplazar el volumen raíz.

El volumen raíz de reemplazo obtiene el mismo tipo de volumen y atributo de eliminación al terminar que el volumen raíz original. También obtiene el tamaño de la asignación de dispositivos de bloques del volumen raíz de la AMI.

> **Note**
>
> El tamaño de la asignación de dispositivos de bloques del volumen raíz de la AMI debe ser igual o mayor que el tamaño del volumen raíz original. Si el tamaño de la asignación de dispositivos de bloques del volumen raíz de la AMI es menor que el tamaño del volumen raíz original, se producirá un error en la solicitud.

Una vez finalizada la tarea de reemplazo del volumen raíz, la siguiente información nueva y actualizada se refleja al describir la instancia mediante la consola, la AWS CLI o los SDK de AWS:

- Nuevo ID de AMI
- Nuevo ID de volumen del volumen raíz
- Configuración del modo de arranque actualizada (si la AMI la modificó)
- Configuración de NitroTPM actualizada (si la AMI lo habilitó)
- Configuración de ENA actualizada (si la AMI lo habilitó)
- Configuración de sriov-net actualizada (si la AMI lo habilitó)

El nuevo ID de la AMI también se refleja en los metadatos de la instancia.

Consideraciones para utilizar una AMI:

- Si usa una AMI que tiene varias asignaciones de dispositivos de bloques, solo se usará el volumen raíz de la AMI. Los demás volúmenes (que no son raíz) se ignoran.
- Solo puede utilizar esta función si tiene permisos para la AMI y la instantánea del volumen raíz asociada. No puede utilizar esta función con las AMI de AWS Marketplace.
- Solo puede usar una AMI sin un código de producto si la instancia tampoco lo tiene.
- El tamaño de la asignación de dispositivos de bloques del volumen raíz de la AMI debe ser igual o mayor que el tamaño del volumen raíz original. Si el tamaño de la asignación de dispositivos de bloques del volumen raíz de la AMI es menor que el tamaño del volumen raíz original, se producirá un error en la solicitud.
- Los documentos de identidad de la instancia se actualizan automáticamente.
- Si la instancia admite NitroTPM, los datos de NitroTPM de la instancia se restablecen y se generan nuevas claves.

Reemplazar un volumen raíz

Cuando reemplaza el volumen raíz de una instancia, se crea una tarea de reemplazo del volumen raíz. Puede utilizar la tarea de reemplazo del volumen raíz para supervisar el progreso y el resultado del proceso de reemplazo. Para obtener más información, consulte Ver tareas de reemplazo de volumen raíz.

Puede reemplazar el volumen raíz de una instancia mediante uno de los métodos siguientes.

> **Note**
>
> Si utiliza la consola de Amazon EC2, la funcionalidad solo está disponible en la consola nueva.

New console

Para reemplazar el volumen raíz

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancias).

3. Seleccione la instancia para la que desea reemplazar el volumen raíz y elija Acciones, Monitorear y solucionar problemas, Reemplazar volumen raíz.

> **Note**
>
> La acción Reemplazar volumen raíz estará desactivada si la instancia seleccionada no está en estado de `running`.

4. En la pantalla Reemplazar volumen raíz, realice una de las acciones siguientes:

   - Para restaurar el volumen raíz de reemplazo su estado de inicialización inicial, elija Crear tarea de sustitución sin seleccionar ninguna instantánea.
   - Para restaurar el volumen raíz de reemplazo en una instantánea específica, en Instantánea, seleccione la instantánea que desea utilizar y, a continuación, elija Crear tarea de sustitución.
   - Para restaurar el volumen raíz de reemplazo mediante una AMI, en AMI, seleccione la AMI que va a usar y, a continuación, elija Crear tarea de sustitución.

5. Para eliminar el volumen raíz original una vez finalizada la tarea de reemplazo, seleccione Eliminar el volumen raíz reemplazado.

AWS CLI

Para restaurar el volumen raíz de reemplazo al estado de inicialización inicial

Utilice el comando create-replace-root-volume-task. En `--instance-id`, especifique el ID de la instancia para la que desea reemplazar el volumen raíz. Omita los parámetros `--snapshot-id` e `--image-id`. Para eliminar el volumen raíz original después de haberlo reemplazado, incluya `--delete-replaced-root-volume` y especifique `true`.

```
$ aws ec2 create-replace-root-volume-task \
--instance-id i-1234567890abcdef0 \
--delete-replaced-root-volume true
```

Para restaurar el volumen raíz de reemplazo a una instantánea específica

Utilice el comando create-replace-root-volume-task. En `--instance-id`, especifique el ID de la instancia para la que desea reemplazar el volumen raíz. En `--snapshot-id`, especifique el

ID de la instantánea que se va a usar. Para eliminar el volumen raíz original después de haberlo reemplazado, incluya `--delete-replaced-root-volume` y especifique `true`.

```
$ aws ec2 create-replace-root-volume-task \
--instance-id i-1234567890abcdef0 \
--snapshot-id snap-9876543210abcdef0 \
--delete-replaced-root-volume true
```

Para restaurar el volumen raíz de reemplazo mediante una AMI

Utilice el comando create-replace-root-volume-task. En `--instance-id`, especifique el ID de la instancia para la que desea reemplazar el volumen raíz. En `--image-id`, especifique el ID de la AMI que quiere usar. Para eliminar el volumen raíz original después de haberlo reemplazado, incluya `--delete-replaced-root-volume` y especifique `true`.

```
$ aws ec2 create-replace-root-volume-task \
--instance-id i-01234567890abcdef \
--image-id ami-09876543210abcdef \
--delete-replaced-root-volume true
```

Tools for Windows PowerShell

Para restaurar el volumen raíz de reemplazo al estado de inicialización inicial

Utilice el comando New-EC2ReplaceRootVolumeTask. En `-InstanceId`, especifique el ID de la instancia para la que desea reemplazar el volumen raíz. Omita los parámetros `-SnapshotId` e `-ImageId`. Para eliminar el volumen raíz original después de haberlo reemplazado, incluya `-DeleteReplacedRootVolume` y especifique `$true`.

```
PS C:\> New-EC2ReplaceRootVolumeTask -InstanceId i-1234567890abcdef0 -
DeleteReplacedRootVolume $true
```

Para restaurar el volumen raíz de reemplazo a una instantánea específica

Utilice el comando New-EC2ReplaceRootVolumeTask. En `--InstanceId`, especifique el ID de la instancia para la que desea reemplazar el volumen raíz. En `-SnapshotId`, especifique el ID de la instantánea que se va a usar. Para eliminar el volumen raíz original después de haberlo reemplazado, incluya `-DeleteReplacedRootVolume` y especifique `$true`.

```
PS C:\> New-EC2ReplaceRootVolumeTask -InstanceId i-1234567890abcdef0 -
SnapshotId snap-9876543210abcdef0 -DeleteReplacedRootVolume $true
```

Para restaurar el volumen raíz de reemplazo mediante una AMI

Utilice el comando New-EC2ReplaceRootVolumeTask. En `-InstanceId`, especifique el ID de la instancia para la que desea reemplazar el volumen raíz. En `-ImageId`, especifique el ID de la AMI que quiere usar. Para eliminar el volumen raíz original después de haberlo reemplazado, incluya `-DeleteReplacedRootVolume` y especifique `$true`.

```
PS C:\> New-EC2ReplaceRootVolumeTask -InstanceId i-1234567890abcdef0 -
ImageId ami-09876543210abcdef -DeleteReplacedRootVolume $true
```

Ver tareas de reemplazo de volumen raíz

Cuando reemplaza el volumen raíz de una instancia, se crea una tarea de reemplazo del volumen raíz. La tarea de sustitución del volumen raíz pasa por los siguientes estados durante el proceso:

- `pending`: el volumen de reemplazo está en creación.
- `in-progress`: se desvincula el volumen original y se asocia el volumen de reemplazo.
- `succeeded`: se ha asociado el volumen de reemplazo a la instancia correctamente y la instancia está disponible.
- `failing`: la tarea de reemplazo está en proceso de fallar.
- `failed`: se produjo un error en la tarea de reemplazo, pero el volumen raíz original aún está asociado.
- `failing-detached`: la tarea de reemplazo está en proceso de error y es posible que la instancia no tenga un volumen raíz asociado.
- `failed-detached`: se produjo un error en la tarea de reemplazo y la instancia no tiene un volumen raíz asociado.

Puede ver las tareas de reemplazo de volumen raíz de una instancia mediante uno de los métodos siguientes.

> **Note**
>
> Si utiliza la consola de Amazon EC2, la funcionalidad solo está disponible en la consola nueva.

Console

Para ver las tareas de reemplazo de volumen raíz

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancias).
3. Seleccione la instancia para la que desea ver las tareas de reemplazo de volumen raíz y, a continuación, elija la pestaña Almacenamiento.
4. En la pestaña Almacenamiento, expanda Tareas de reemplazo de volumen raíz recientes.

AWS CLI

Para ver el estado de una tarea de reemplazo de volumen raíz

Utilice el comando describe-replace-root-volume-tasks y especifique los ID de las tareas de reemplazo de volumen raíz que se van a ver.

```
$ aws ec2 describe-replace-root-volume-tasks \
--replace-root-volume-task-ids replacevol-1234567890abcdef0
```

```
{
  "ReplaceRootVolumeTasks": [
  {
    "ReplaceRootVolumeTaskId": "replacevol-1234567890abcdef0",
    "InstanceId": "i-1234567890abcdef0",
    "TaskState": "succeeded",
    "StartTime": "2020-11-06 13:09:54.0",
    "CompleteTime": "2020-11-06 13:10:14.0",
    "SnapshotId": "snap-01234567890abcdef",
    "DeleteReplacedRootVolume": "True"
  }]
}
```

También puede especificar el filtro `instance-id` para filtrar los resultados por instancia.

```
$ aws ec2 describe-replace-root-volume-tasks \
--filters Name=instance-id,Values=i-1234567890abcdef0
```

Tools for Windows PowerShell

Para ver el estado de una tarea de reemplazo de volumen raíz

Utilice el comando Get-EC2ReplaceRootVolumeTask y especifique los ID de las tareas de reemplazo de volumen raíz que se van a ver.

```
PS C:\> Get-EC2ReplaceRootVolumeTask -
ReplaceRootVolumeTaskIds replacevol-1234567890abcdef0
```

También puede especificar el filtro `instance-id` para filtrar los resultados por instancia.

```
PS C:\> Get-EC2ReplaceRootVolumeTask -Filters @{Name = 'instance-id'; Values =
 'i-1234567890abcdef0'} | Format-Table
```

Nombres de dispositivos en las instancias de Amazon EC2

Cuando adjunta un volumen a su instancia, incluye un nombre de dispositivo para el volumen. Amazon EC2 utiliza este nombre del dispositivo. El controlador del dispositivo de bloques de la instancia asigna el nombre del volumen real al montar el volumen, y el nombre asignado puede diferir del que Amazon EC2 usa.

El número de volúmenes que puede admitir la instancia se establece en función del sistema operativo. Para obtener más información, consulte Límites de volumen de instancias.

Contenido

Nombres de dispositivos disponibles

instancias de Linux

Las instancias de Linux tienen a su disposición dos tipos de virtualización: paravirtual (PV) o máquina virtual de hardware (HVM). El tipo de virtualización de una instancia se determina en función de la AMI utilizada para iniciarla. Todos los tipos de instancias admiten AMI HVM. Algunos tipos de instancia de generaciones anteriores admiten AMI paravirtuales (PV). Asegúrese de tomar nota del tipo de virtualización de su AMI, ya que los nombres de dispositivos recomendados y disponibles que puede utilizar dependen del tipo de virtualización de su instancia. Para obtener más información, consulte Tipos de virtualización de AMI.

En la siguiente tabla, se muestran los nombres de dispositivo disponibles que puede especificar en una asignación de dispositivos de bloques o al adjuntar un volumen de EBS.

Tipo de virtualización	Disponible	Reservado para volumen raíz	Recomendado para volúmenes EBS	Volúmenes de almacén de instancias
Paravirtual	/dev/sd[a-z] /dev/sd[a-z][1-15] /dev/hd[a-z] /dev/hd[a-z][1-15]	/dev/sda1	/dev/sd[f-p] /dev/sd[f-p][1-6]	/dev/sd[b-e]
HVM	/dev/sd[a-z] /dev/xvd[a-d][a-z] /dev/xvd[e-z]	Difiere por AMI /dev/sda1 o /dev/xvda	/dev/sd[f-p] *	/dev/sd[b-e] /dev/sd[b-h] (h1.16xlarge) /dev/sd[b-y] (d2.8xlarge) /dev/sd[b-i] (i2.8xlarge)

Tipo de virtualización	Disponible	Reservado para volumen raíz	Recomendado para volúmenes EBS	Volúmenes de almacén de instancias
				**

* Los nombres de dispositivos que especifica para los volúmenes de EBS NVMe en una asignación de dispositivos de bloques se cambian por los nombres de dispositivos NVMe (`/dev/nvme[0-26]n1`). El controlador de dispositivo de bloques puede asignar nombres de dispositivos NVMe en un orden distinto al especificado para los volúmenes de la asignación de dispositivos de bloques.

** Los volúmenes de almacén de instancias NVMe se enumeran automáticamente y se les asigna un nombre de dispositivo NVMe.

instancias de Windows

Las AMI de Windows utilizan uno de los siguientes conjuntos de controladores para permitir el acceso al hardware virtualizado: AWS PV, Citrix PV y RedHat PV. Para obtener más información, consulte the section called “Controladores PV de Windows”.

En la siguiente tabla, se muestran los nombres de dispositivo disponibles que puede especificar en una asignación de dispositivos de bloques o al adjuntar un volumen de EBS.

Tipo de controlador	Disponible	Reservado para volumen raíz	Recomendado para volúmenes EBS	Volúmenes de almacén de instancias
AWS PV, Citrix PV	xvd[b-z] xvd[b-c][a-z] /dev/sda1 /dev/sd[b-e]	/dev/sda1	xvd[f-z] *	xvdc[a-x] xvd[a-e] **
Red Hat PV	xvd[a-z] xvd[b-c][a-z]	/dev/sda1	xvd[f-p]	xvdc[a-x] xvd[a-e]

Tipo de controlador	Disponible	Reservado para volumen raíz	Recomendado para volúmenes EBS	Volúmenes de almacén de instancias
	/dev/sda1 /dev/sd[b-e]			

* Para Citrix PV y Red Hat PV, si asigna un volumen de EBS con el nombre `xvda`, Windows no reconoce el volumen (este es visible para AWS PV o AWS NVMe).

** Se enumera y se asigna automáticamente una letra de unidad de Windows a los volúmenes de almacén de instancias NVMe.

Para obtener más información acerca de los volúmenes del almacén de instancias, consulte Almacén de instancias Amazon EC2. Para obtener más información acerca de los volúmenes NVMe EBS (instancias basadas en Nitro), incluida la forma de identificar el dispositivo EBS, consulte Amazon EBS y NVMe en la Guía del usuario de Amazon EBS.

Consideraciones sobre el nombre de los dispositivos

Tenga en cuenta las siguientes consideraciones cuando seleccione un nombre de dispositivo:

- Aunque puede adjuntar volúmenes EBS utilizando los nombres de dispositivo usados para adjuntar volúmenes de almacén de instancias, le recomendamos que no lo haga porque el comportamiento puede ser impredecible.
- El número de los volúmenes de almacén de instancias de NVMe de una instancia varía según el tamaño de la instancia. A los volúmenes de almacén de instancias NVMe se les enumera y se les asigna automáticamente un nombre de dispositivo NVMe (instancias de Linux) o una letra de unidad de Windows (instancias de Windows).
- (Instancias de Windows) Las AMI de Windows de AWS incluyen software adicional que prepara la instancia cuando se arranca por primera vez. Este puede ser el servicio EC2Config (las AMI para Windows anteriores a Windows Server 2016) o EC2Launch (Windows Server 2016 y versiones posteriores). Una vez que se han asignado los dispositivos a las unidades, se inicializan y se montan. La unidad raíz se inicializa y monta como `C:\`. De forma predeterminada, cuando un volumen de EBS se adjunta a una instancia de Windows, se puede mostrar como cualquier letra de unidad en la instancia. Puede cambiar la configuración para establecer las letras de unidad de los volúmenes según sus especificaciones. Para volúmenes del almacén de instancias, la opción

predeterminada depende del controlador. AWS Los controladores PV y Citrix PV asignan a los volúmenes de almacén de instancias letras de unidad de la Z: a la A:. Los controladores Red Hat asignan a los volúmenes de almacén de instancias letras de unidad de la D: a la Z:. Para obtener más información, consulte Configuración de la inicialización de instancias de Windows de Amazon EC2 y Asignar discos a volúmenes en instancia de Windows.

- (Instancias de Linux) En función de la unidad de dispositivo de bloques del kernel, el dispositivo puede ir asociado a otro nombre diferente del especificado. Por ejemplo, si especifica un nombre de dispositivo de `/dev/sdh`, se podría cambiar el nombre del dispositivo por `/dev/xvdh` o `/dev/hdh`. En muchos casos, la letra final continúa siendo la misma. En algunas versiones de Red Hat Enterprise Linux (y sus variantes como CentOS), podría cambiar también la letra final (`/dev/sda` puede convertirse en `/dev/xvde`). En estos casos, la letra final de cada nombre del dispositivo se aumenta el mismo número de veces. Por ejemplo, si se cambia el nombre de `/dev/sdb` a `/dev/xvdf`, entonces se cambia el nombre de `/dev/sdc` a `/dev/xvdg`. Amazon Linux crea un enlace simbólico para el nombre que especificó para el dispositivo cuyo nombre cambió. Es posible que otros sistemas operativos se comporten de otra forma.
- (Instancias de Linux) Las AMI de HVM no admiten el uso de números finales en los nombres de dispositivos, salvo `/dev/sda1`, que es el nombre de dispositivo reservado para el dispositivo raíz, y `/dev/sda2`. Aunque es posible utilizar `/dev/sda2`, no se recomienda usar este mapeo de dispositivo con instancias HVM.
- (Instancias de Linux) Cuando se utilizan AMI PV, no se pueden asociar volúmenes que compartan las mismas letras de dispositivo, tanto con dígitos finales como sin ellos. Por ejemplo, si adjunta un volumen como `/dev/sdc` y otro volumen como `/dev/sdc1`, solo `/dev/sdc` será visible para la instancia. Para utilizar dígitos finales en nombres de dispositivos, debe usar dígitos finales en todos los nombres de dispositivos que compartan las mismas letras de base (como `/dev/sdc1`, `/dev/sdc2`, `/dev/sdc3`).
- (Instancias de Linux) Puede que algunos kernels personalizados tengan restricciones que limiten el uso a `/dev/sd[f-p]` o `/dev/sd[f-p][1-6]`. Si tiene problemas para usar `/dev/sd[q-z]` o `/dev/sd[q-z][1-6]`, intente cambiar a `/dev/sd[f-p]` o `/dev/sd[f-p][1-6]`.

Antes de especificar el nombre del dispositivo que ha seleccionado, compruebe que esté disponible. De lo contrario, obtendrá un error que indica que el nombre del dispositivo ya está en uso. Para ver los dispositivos de disco y sus puntos de montaje, utilice el comando lsblk (instancias de Linux), la utilidad de administración de discos o el comando diskpart (instancias de Windows).

Mapeos de dispositivos de bloques

Cada instancia que lance tiene un volumen de dispositivo raíz asociado, que puede ser un volumen de Amazon EBS o un volumen de almacén de instancias. Puede utilizar la asignación de dispositivos de bloques para especificar los volúmenes de EBS adicionales o volúmenes de almacén de instancias para adjuntar a una instancia a la hora de iniciarla. También se pueden asociar volúmenes de EBS adicionales a una instancia en ejecución. Sin embargo, la única forma de adjuntar volúmenes de almacén de instancias a una instancia es utilizar la asignación de dispositivos de bloques para adjuntarlos a los volúmenes al iniciar dicha instancia.

Contenido

Conceptos sobre la asignación de dispositivos de bloques

Un dispositivo de bloques es un dispositivo de almacenamiento que traslada los datos en secuencias bytes o bits (bloques). Estos dispositivos admiten el acceso aleatorio y, por lo general, usan E/S en búfer. Entre los ejemplos de este tipo de dispositivos se incluyen los discos duros, las unidades de CD-ROM y las memorias flash. Un dispositivo de bloques se puede conectar físicamente a un equipo o bien se puede obtener acceso a él de forma remota como si estuviera conectado físicamente al equipo.

Amazon EC2 admite dos tipos de dispositivo de bloques:

- Volúmenes de almacén de instancias (dispositivos virtuales cuyo hardware subyacente está conectado físicamente al equipo host de la instancia)
- Volúmenes de EBS (dispositivos de almacenamiento remoto)

Una asignación de dispositivos de bloques define los dispositivos de bloques (volúmenes de almacén de instancias y volúmenes de EBS) que se deben asociar a la instancia. Puede especificar una asignación de dispositivos de bloques como parte la creación de una AMI para que el mapeo sea utilizado por todas las instancias que se lancen desde la AMI. También puede especificar una asignación de dispositivos de bloques cuando se inicia una instancia, de forma que este mapeo anula al especificado en la AMI desde la que se lanzó la instancia. Tenga en cuenta que todos

los volúmenes de almacenes de instancias NVMe admitidos por un tipo de instancia se enumeran automáticamente y se les asigna un nombre de dispositivo al iniciar la instancia; su inclusión en la asignación de dispositivos de bloques no tiene ningún efecto.

Contenido

Entradas de asignación de dispositivos de bloques

Cuando crea una asignación de dispositivos de bloques, se especifica la siguiente información para cada dispositivo de bloques que necesita adjuntar a la instancia:

- El nombre del dispositivo utilizado dentro de Amazon EC2. El controlador del dispositivo de bloques de la instancia asigna el nombre real del volumen al montarlo. El nombre asignado puede ser distinto al nombre recomendado por Amazon EC2. Para obtener más información, consulte Nombres de dispositivos en las instancias de Amazon EC2.

Para volúmenes de almacén de instancias, también se especifica la siguiente información:

- El dispositivo virtual: `ephemeral[0-23]`. Tenga en cuenta que el número y el tamaño de los volúmenes de almacén de instancias disponibles para la instancia varía según el tipo de instancia.

Para volúmenes de almacenamiento de instancias NVMe, también se aplica la siguiente información:

- Estos volúmenes se enumeran automáticamente y se les asigna un nombre de dispositivo; su inclusión en la asignación de dispositivos de bloques no tiene ningún efecto.

Para los volúmenes de EBS, también debe especificar la siguiente información:

- El ID de la instantánea que se utiliza para crear el dispositivo de bloques (snap-xxxxxxxx). Este valor es opcional siempre que especifique un tamaño de volumen. No se puede especificar el ID de una instantánea archivada.

- El tamaño del volumen, en GiB. El tamaño especificado debe ser superior o igual al tamaño de la instantánea especificada.
- Si se elimina el volumen de la terminación de instancias (`true` o `false`). El valor predeterminado es `true` para el volumen de dispositivo raíz y `false` para volúmenes adjuntos. Al crear una AMI, su asignación de dispositivos de bloques hereda esta configuración de la instancia. Al iniciar una instancia, hereda esta configuración de la AMI.
- El tipo de volumen, que puede ser `gp2` y `gp3` para los SSD de uso general, `io1` e `io2` para los SSD de IOPS aprovisionadas, `st1` para los HDD con rendimiento optimizado, `sc1` para los HDD en frío o `standard` para los magnéticos.
- El número de operaciones de entrada/salida por segundo (IOPS) que admite el volumen. (Se utiliza solo con volúmenes `io1` e `io2`).

Advertencias del almacén de instancias de la asignación de dispositivos de bloques

Existen varias salvedades que se deben tener en cuenta a la hora de iniciar instancias con AMIs que tienen volúmenes de almacén de instancias en sus mapeos de dispositivos de bloques.

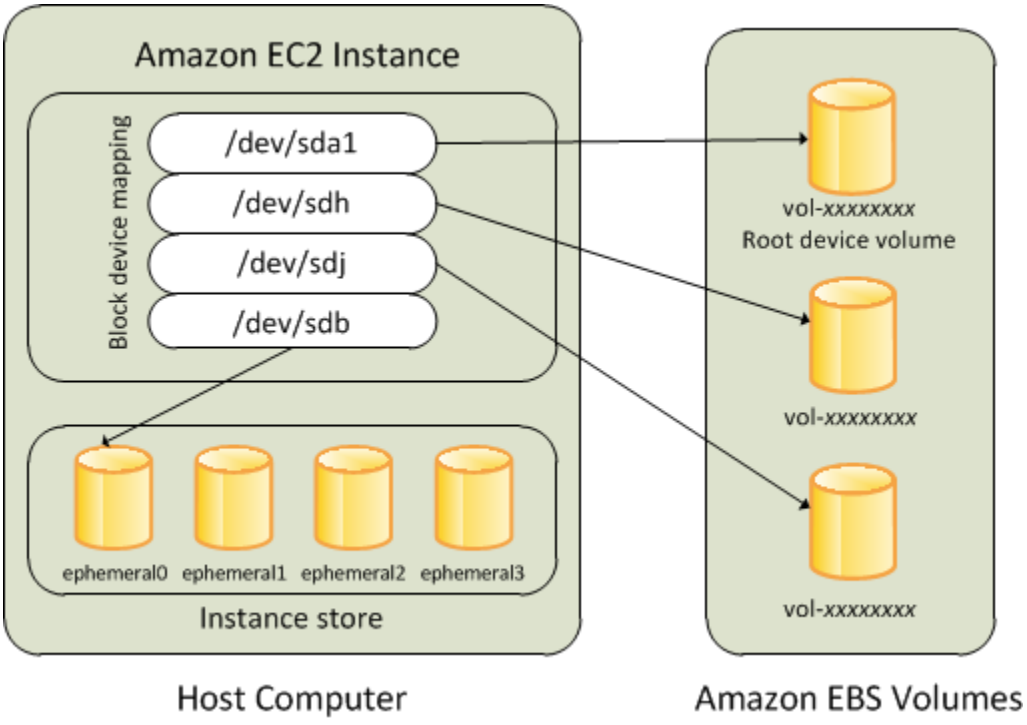
- Algunos tipos de instancia incluyen más volúmenes de almacén de instancias que otros, mientras que algunos tipos de instancia no contienen ninguno. Si su tipo de instancia admite un volumen de almacén de instancias y la AMI tiene mapeos para dos volúmenes de almacén de instancias, la instancia se inicia con uno solo.
- Los volúmenes de almacén de instancias solo se pueden mapear durante la inicialización. No puede parar una instancia sin volúmenes de almacén de instancias (como `t2.micro`), cambie la instancia a un tipo que admita volúmenes de almacén de instancias y, a continuación, reinicie la instancia con volúmenes de almacén de instancias. Sin embargo, puede crear una AMI desde la instancia y iniciarla en un tipo de instancia que admita volúmenes de almacén de instancias y, a continuación, mapear dichos volúmenes de almacén de instancias en la instancia.
- Si inicia una instancia con volúmenes de almacén de instancias mapeados y, a continuación, para la instancia, la cambia por un tipo de instancia con menos volúmenes de almacén de instancias y, a continuación, la reinicia, los mapeos de los volúmenes de almacén de instancias de la inicialización inicial seguirán mostrándose en los metadatos de la instancia. Sin embargo, solo estará disponible para la instancia el número máximo de volúmenes de almacén de instancias admitido para ese tipo de instancia.

> **Note**
>
> Cuando se para una instancia, se pierden todos los datos de los volúmenes de almacén de instancias.

- Dependiendo de la capacidad del almacén de instancias en el momento de la inicialización, las instancias M3 podrían omitir los mapeos de dispositivos de bloques del almacén de instancias de la AMI durante la inicialización, salvo que se especifiquen en se momento. Debe especificar las asignaciones de dispositivos de bloques del almacén de instancias en el momento de la inicialización, incluso si la AMI que va a iniciar tiene los volúmenes de almacén de instancias mapeados en la AMI, para garantizar que los volúmenes de almacén de instancias estén disponibles cuando se lance la instancia.

Ejemplos de asignación de dispositivos de bloques

Esta figura muestra un ejemplo de asignación de dispositivos de bloques para una instancia respaldada por EBS. Mapea `/dev/sdb` en `ephemeral0` y mapea dos volúmenes de EBS, un en `/dev/sdh` y el otro en `/dev/sdj`. También muestra el volumen de EBS que es el volumen de dispositivo raíz, `/dev/sda1`.



Tenga en cuenta que este ejemplo de asignación de dispositivos de bloques se utiliza en los comandos y API de muestra de este tema. Puede encontrar comandos y API de muestra que crean asignaciones de dispositivos de bloques en Especificar una asignación de dispositivos de bloques para una AMI y Actualizar la asignación de dispositivos de bloques al iniciar una instancia.

Disponibilidad de los dispositivos en el sistema operativo

Amazon EC2 utiliza nombres como `/dev/sdh` y `xvdh` para describir dispositivos de bloques. Amazon EC2 utiliza la asignación de dispositivos de bloques para especificar los dispositivos de bloques que se deben adjuntar a una instancia de EC2. Cuando un dispositivo de bloques se adjunta a una instancia, debe ser montado por el sistema operativo antes de que se pueda obtener acceso al dispositivo de almacenamiento. Cuando un dispositivo de bloques se separa de una instancia, es desmontado por el sistema operativo y ya no se puede obtener acceso al dispositivo de almacenamiento.

Instancias de Linux: los nombres de dispositivo especificados en la asignación de dispositivos de bloques se mapean en sus dispositivos de bloques correspondientes al arrancar la instancia por primera vez. El tipo de instancia determina qué volúmenes de almacén de instancias se formatean y montan de forma predeterminada. Puede montar volúmenes de almacén de instancias adicionales durante la inicialización siempre que no se supere el número de volúmenes de almacén de instancias disponibles para el tipo de instancia. Para obtener más información, consulte Almacén de instancias Amazon EC2. El controlador del dispositivo de bloques de la instancia determina qué dispositivos se utilizan al formatear y montar los volúmenes.

Instancias de Windows: los nombres de dispositivo especificados en la asignación de dispositivos de bloques se mapean en sus dispositivos de bloques correspondientes al arrancar la instancia por primera vez y, a continuación, el servicio Ec2Config inicializa y monta las unidades. El volumen del dispositivo raíz se monta como `C:\`. Los volúmenes de almacén de instancias se montan como `Z:\`, `Y:\` y así sucesivamente. El volumen de EBS se puede montar en cualquier letra de unidad. Sin embargo, puede configurar la asignación de letras de unidad para volúmenes de EBS. Si desea obtener más información, consulte the section called “Configuración de agentes de inicialización de Windows”.

Asignación de dispositivos de bloques AMI

Cada AMI tiene una asignación de dispositivos de bloques que especifica los dispositivos de bloques que se deben adjuntar a una instancia cuando se inicia desde la AMI. Para añadir más dispositivos de bloques a una AMI, debe crear su propia AMI.

Contenido

Especificar una asignación de dispositivos de bloques para una AMI

Existen dos maneras de especificar volúmenes además del volumen raíz al crear una AMI. Si ya ha adjuntado volúmenes a una instancia en ejecución antes de crear la AMI desde la instancia, la asignación de dispositivos de bloques de la AMI incluye esos mismos volúmenes. Para volúmenes de EBS, los datos existentes se guardan en una nueva instantánea, y es esta instantánea la que se especifica en la asignación de dispositivos de bloques. Para los volúmenes de almacén de instancias, los datos no se conservan.

Para una AMI respaldada por EBS, puede añadir volúmenes de EBS y volúmenes de almacén de instancias mediante una asignación de dispositivos de bloques Para una AMI con respaldo en el almacén de instancias, puede añadir volúmenes de almacén de instancias solo modificando las entradas de la asignación de dispositivos de bloques en el archivo de manifiesto de la imagen al registrar la imagen.

> **Note**
>
> Para instancias M3, debe especificar volúmenes de almacén de instancias en la asignación de dispositivos de bloques para la instancia al iniciarla. Al iniciar una instancia M3, los volúmenes de almacén de instancias especificados en la asignación de dispositivos de bloques de la AMI podrían omitirse si no se han especificado como parte de la asignación de dispositivos de bloques de la instancia.

Console

Para añadir volúmenes a una AMI con la consola

1. Abra la consola de Amazon EC2.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Seleccione una instancia y elija Acciones, Imagen y plantillas, Crear imagen.
4. Introduzca un nombre y una descripción para la imagen.

5. Los volúmenes de instancia aparecen en Volúmenes de instancia. Para agregar otro volumen, elija Agregar volumen.
6. En Tipo de volumen, elija el tipo de volumen. Para Dispositivo, elija el nombre del dispositivo. Para un volumen de EBS, puede especificar detalles adicionales, como una instantánea, tamaño de volumen, tipo de volumen, IOPS y estado de cifrado.
7. Elija Create image (Crear imagen).

Command line

Para añadir volúmenes a una AMI con la línea de comando

Utilice el comando create-image AWS CLI para especificar una asignación de dispositivos de bloques para una AMI respaldada por EBS. Utilice el comando register-image AWS CLI para especificar una asignación de dispositivos de bloques para una AMI con respaldo en el almacén de instancias.

Especifique la asignación de dispositivos de bloques utilizando el parámetro `--block-device-mappings`. Los argumentos cifrados en JSON se pueden administrar de forma directa en la línea de comando o mediante una referencia a un archivo:

```
--block-device-mappings [mapping, ...]
--block-device-mappings [file://mapping.json]
```

Para añadir un volumen de almacén de instancias, utilice el siguiente mapeo:

```
{
    "DeviceName": "device_name",
    "VirtualName": "ephemeral0"
}
```

Para añadir un volumen de gp2 de 100 GiB vacío, utilice el siguiente mapeo:

```
{
    "DeviceName": "device_name",
    "Ebs": {
      "VolumeSize": 100
    }
}
```

Para añadir un volumen EBS basado en una instantánea, utilice el siguiente mapeo:

```
{
    "DeviceName": "device_name",
    "Ebs": {
      "SnapshotId": "snap-xxxxxxxx"
    }
}
```

Para omitir un mapeo para un dispositivo, utilice el siguiente mapeo:

```
{
    "DeviceName": "device_name",
    "NoDevice": ""
}
```

También puede usar el parámetro `-BlockDeviceMapping` con los siguientes comandos (AWS Tools for Windows PowerShell):

- New-EC2Image
- Register-EC2Image

Visualizar los volúmenes de EBS en una asignación de dispositivos de bloques de una AMI

Puede enumerar fácilmente los volúmenes de EBS en la asignación de dispositivos de bloques de una AMI.

Console

Para ver los volúmenes de EBS de una AMI utilizando la consola

1. Abra la consola de Amazon EC2.
2. En el panel de navegación, elija AMIs.
3. Elija Imágenes de EBS en la lista Filtro para obtener una lista de AMI respaldadas por EBS.
4. Seleccione la AMI deseada y compruebe la pestaña Detalles. Como mínimo, se muestra la siguiente información para el dispositivo raíz:

    - Tipo de dispositivo raíz (`ebs`)

- Tipo de dispositivo raíz (por ejemplo, `/dev/sda1`)
- Dispositivo de bloques (por ejemplo, `/dev/sda1=snap-1234567890abcdef0:8:true`)

Si la AMI se creó con volúmenes de EBS adicionales utilizando una asignación de dispositivos de bloques, el campo Dispositivos de bloques muestra también el mapeo de dichos volúmenes adicionales. (Esta pantalla no muestra volúmenes de almacén de instancias).

Command line

Para ver los volúmenes de EBS de una AMI utilizando la línea de comando

Utilice el comando describe-images (AWS CLI) o Get-EC2Image (AWS Tools for Windows PowerShell) para enumerar los volúmenes de EBS de la asignación de dispositivos de bloques de una AMI.

Asignación de dispositivos de bloques de instancias

De forma predeterminada, una instancia que lance incluye cualquier dispositivo de almacenamiento especificado en la asignación de dispositivos de bloques de la AMI desde la que se lanzó la instancia. Puede especificar cambios en la asignación de dispositivos de bloques de una instancia al iniciarla, y estas actualizaciones sobrescriben o se combinan con la asignación de dispositivos de bloques de la AMI.

Limitaciones

- Para el volumen raíz, solo se puede modificar lo siguiente: tamaño del volumen, tipo de volumen y la marca Eliminar al terminar.
- Al modificar un volumen de EBS, no se puede reducir su tamaño. Por lo tanto, debe especificar una instantánea cuyo tamaño sea igual o superior al de la instantánea especificada en la asignación de dispositivos de bloques de la AMI.

Contenido

- Visualizar la asignación de dispositivos de bloques de una instancia para volúmenes de almacén de instancias

Actualizar la asignación de dispositivos de bloques al iniciar una instancia

Puede añadir volúmenes de EBS y volúmenes de almacén de instancias a una instancia al iniciarla. Tenga en cuenta que la actualización de la asignación de dispositivos de bloques de una instancia no realiza cambios permanentes en la asignación de dispositivos de bloques de la AMI desde la que se lanzó.

Console

Para añadir volúmenes a una instancia utilizando la consola

1. Abra la consola de Amazon EC2.
2. En el panel, elija Iniciar instancia.
3. En la página Choose an Amazon Machine Image (AMI) (Elegir una imagen de máquina de Amazon (AMI)), seleccione AMI que desea utilizar y elija Select (Seleccionar).
4. Siga el asistente para completar las páginas Elegir un tipo de instancia y Configurar detalles de instancia.
5. En la página Agregar almacenamiento, puede modificar el volumen raíz, los volúmenes de EBS y los volúmenes almacén de instancias del modo siguiente:
   - Para cambiar el tamaño del volumen raíz, localice el volumen Raíz en la columna Tipo y cambie el campo Tamaño.
   - Para suprimir un volumen de EBS especificado en la asignación de dispositivos de bloques de la AMI utilizada para iniciar la instancia, localice dicho volumen y haga clic en el icono Eliminar.
   - Para agregar un volumen de EBS, elija Agregar nuevo volumen y luego EBS en la lista Tipo; después, rellene los campos (Dispositivo, Instantánea, y así sucesivamente).
   - Para suprimir un volumen de almacén de instancias especificado en el asignación de dispositivos de bloques de la AMI utilizada para iniciar la instancia, localice dicho volumen y elija el icono Eliminar.
   - Para añadir un volumen de almacén de instancias, elija Añadir nuevo volumen, seleccione Almacén de instancias en la lista Tipo y seleccione un nombre de dispositivo en Dispositivo.

6. Complete las páginas del asistente restantes y elija Iniciar.

Command line

Para agregar volúmenes a una instancia utilizando la AWS CLI

Utilice el comando run-instances de la AWS CLI con la opción `--block-device-mappings` para especificar una asignación de dispositivos de bloques para una instancia en el momento de la inicialización.

Por ejemplo, supongamos que una AMI respaldada por EBS especifica la siguiente asignación de dispositivos de bloques para una instancia de Linux:

- `/dev/sdb` = `ephemeral0`
- `/dev/sdh` = `snap-1234567890abcdef0`
- `/dev/sdj` = `100`

Para evitar que `/dev/sdj` se adjunte a una instancia iniciada desde esta AMI, utilice el siguiente mapeo.

```
{
    "DeviceName": "/dev/sdj",
    "NoDevice": ""
}
```

Para aumentar el tamaño de `/dev/sdh` a `300 GiB`, especifique el siguiente mapeo. Observe que no es necesario especificar el ID de instantánea de `/dev/sdh`, porque basta especificar el nombre de dispositivo para identificar el volumen.

```
{
    "DeviceName": "/dev/sdh",
    "Ebs": {
      "VolumeSize": 300
    }
}
```

Para aumentar el tamaño del volumen raíz al iniciar la instancia, primero llame a describe-images con el ID de la AMI para verificar el nombre del dispositivo del volumen raíz. Por ejemplo,

`"RootDeviceName": "/dev/xvda"`. Para anular el tamaño del volumen raíz, especifique el nombre del dispositivo raíz utilizado por la AMI y el nuevo tamaño del volumen.

```
{
    "DeviceName": "/dev/xvda",
    "Ebs": {
      "VolumeSize": 100
    }
}
```

Para adjuntar un volumen de almacén de instancias adicional, `/dev/sdc`, especifique el siguiente mapeo. Si el tipo de instancia no admite varios volúmenes de almacén de instancias, este mapeo no tiene ningún efecto. Si la instancia admite volúmenes de almacén de instancias NVMe, se enumeran automáticamente y se les asigna un nombre de dispositivo NVMe.

```
{
    "DeviceName": "/dev/sdc",
    "VirtualName": "ephemeral1"
}
```

Para agregar volúmenes a una instancia utilizando la AWS Tools for Windows PowerShell

Utilice el parámetro `-BlockDeviceMapping` con el comando New-EC2Instance (AWS Tools for Windows PowerShell)

Actualizar la asignación de dispositivos de bloques de una instancia en ejecución

Puede utilizar el comando modify-instance-attribute de la AWS CLI para actualizar la asignación de dispositivos de bloques de una instancia en ejecución. No es necesario parar la instancia antes de cambiar este atributo.

```
aws ec2 modify-instance-attribute --instance-id i-1a2b3c4d --block-device-mappings
 file://mapping.json
```

Por ejemplo, para conservar el volumen raíz en el momento de la terminación de la instancia, especifique lo siguiente en `mapping.json`.

```
[
```

```
  {
    "DeviceName": "/dev/sda1",
    "Ebs": {
      "DeleteOnTermination": false
    }
  }
]
```

También puede usar el parámetro `-BlockDeviceMapping` con el comando Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell).

Visualizar los volúmenes de EBS en la asignación de dispositivos de bloques de una instancia

Puede enumerar fácilmente los volúmenes de EBS mapeados en una instancia.

> **Note**
>
> Para las instancias iniciadas antes de la publicación de la API el 31/10/2009, AWS no puede mostrar la asignación de dispositivos de bloques. Para que AWS pueda mostrar la asignación de dispositivos de bloques, debe desvincular y volver a vincular los volúmenes.

Console

Para ver los volúmenes de EBS de una instancia utilizando la consola

1. Abra la consola de Amazon EC2.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. En la casilla de búsqueda, escriba Tipo de dispositivo raíz y, a continuación, elija EBS. Para mostrar una lista de instancias respaldadas por EBS.
4. Seleccione la instancia deseada y compruebe los detalles que se muestran en la pestaña Almacenamiento. Como mínimo, se muestra la siguiente información para el dispositivo raíz:
   - Tipo de dispositivo raíz (por ejemplo, EBS)
   - Nombre de dispositivo raíz (por ejemplo, `/dev/xvda`)
   - Dispositivos de bloques (por ejemplo, `/dev/xvda`, `/dev/sdf` y `/dev/sdj`)

Si la instancia se inició con volúmenes EBS adicionales mediante una asignación de dispositivos de bloques, aparecerán en Dispositivos de bloques. Los volúmenes de almacén de instancias no aparecen en esta pestaña.

5. Para mostrar información adicional sobre un volumen de EBS, elija su ID de volumen para ir a la página del volumen.

Command line

To view the EBS volumes for an instance using the command line (Para ver los volúmenes de EBS de una instancia utilizando la línea de comando)

Utilice el comando describe-instances (AWS CLI) o Get-EC2Instance (AWS Tools for Windows PowerShell) para enumerar los volúmenes de EBS de la asignación de dispositivos de bloques de una instancia.

Visualizar la asignación de dispositivos de bloques de una instancia para volúmenes de almacén de instancias

El tipo de instancia determina el número y el tipo de volúmenes del almacén de instancias que están disponibles para la instancia. Si el número de volúmenes de almacén de instancias en una asignación de dispositivo de bloque excede el número de volúmenes de almacén de instancias disponible para una instancia, los volúmenes adicionales se ignoran. Para ver los volúmenes de almacén de instancias de su instancia, ejecute el comando lsblk (instancias de Linux) o abra la administración de discos de Windows (instancias de Windows). Para saber cuántos volúmenes de almacén de instancias admite cada tipo de instancia, consulte Especificaciones de tipos de instancias de Amazon EC2.

Cuando visualiza la asignación de dispositivos de bloques para la instancia, solo se ven los volúmenes de EBS, no los volúmenes de almacén de instancias. El método que se utiliza para ver los volúmenes de almacén de instancias de la instancia depende del tipo de volumen.

Volúmenes de almacén de instancias de NVMe

instancias de Linux

Puede usar el paquete de línea de comandos de NVMe, nvme-cli, para consultar los volúmenes de almacén de instancias de NVMe en la asignación de dispositivos de bloques. Descargue e instale el paquete en su instancia y, luego, ejecute el comando siguiente.

```
[ec2-user ~]$ sudo nvme list
```

El siguiente es un resultado de ejemplo para una instancia. El texto de la columna Modelo indica si el volumen es un volumen de EBS o un volumen de almacén de instancias. En este ejemplo, tanto `/dev/nvme1n1` como `/dev/nvme2n1` son volúmenes de almacén de instancias.

```
Node             SN                   Model
 Namespace
---------------- -------------------- ----------------------------------------
 ---------
/dev/nvme0n1     vol06afc3f8715b7a597 Amazon Elastic Block Store              1

/dev/nvme1n1     AWS2C1436F5159EB6614 Amazon EC2 NVMe Instance Storage        1

/dev/nvme2n1     AWSB1F4FF0C0A6C281EA Amazon EC2 NVMe Instance Storage        1
  ...
```

instancias de Windows

Puede usar Administración de discos o PowerShell para enumerar volúmenes de almacén de instancias tanto de EBS como de NVMe. Para obtener más información, consulte the section called “Listar volúmenes NVMe”.

Volúmenes de almacén de instancias de HDD o SSD

Puede usar metadatos de instancia para consultar los volúmenes de almacén de instancias de HDD o SSD en la asignación de dispositivos de bloques. Los volúmenes del almacén de instancias NVMe no se incluyen.

El URI base para todas las solicitudes de metadatos de instancias es `http://169.254.169.254/latest/`. Para obtener más información, consulte Trabajar con metadatos de instancias.

instancias de Linux

En primer lugar, conéctese a la instancia en ejecución. En la instancia, utilice esta consulta para obtener su asignación de dispositivos de bloques.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/block-device-mapping/
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/block-device-mapping/
```

La respuesta incluye los nombres de los dispositivo de bloques de la instancia. Por ejemplo, el resultado para una instancia `m1.small` con respaldo en el almacén de instancias tiene este aspecto.

```
ami
ephemeral0
root
swap
```

El dispositivo `ami` es el dispositivo raíz como indica la instancia. Los volúmenes de almacén de instancias se llaman `ephemeral[0-23]`. El dispositivo `swap` es para el archivo de la página. Si también ha mapeado volúmenes de EBS, estos aparecen como `ebs1` y `ebs2` así sucesivamente.

Para obtener detalles acerca de dispositivo de bloques individual en la asignación de dispositivos de bloques, anexe su nombre a la consulta anterior, tal y como se muestra aquí.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/block-device-mapping/ephemeral0
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/block-device-mapping/
ephemeral0
```

instancias de Windows

En primer lugar, conéctese a la instancia en ejecución. En la instancia, utilice esta consulta para obtener su asignación de dispositivos de bloques.

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/block-device-
mapping/
```

La respuesta incluye los nombres de los dispositivo de bloques de la instancia. Por ejemplo, el resultado para una instancia `m1.small` con respaldo en el almacén de instancias tiene este aspecto.

```
ami
ephemeral0
root
swap
```

El dispositivo `ami` es el dispositivo raíz como indica la instancia. Los volúmenes de almacén de instancias se llaman `ephemeral[0-23]`. El dispositivo `swap` es para el archivo de la página. Si también ha mapeado volúmenes de EBS, estos aparecen como `ebs1` y `ebs2` así sucesivamente.

Para obtener detalles acerca de dispositivo de bloques individual en la asignación de dispositivos de bloques, anexe su nombre a la consulta anterior, tal y como se muestra aquí.

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/block-device-
mapping/ephemeral0
```

Asignar discos a volúmenes en instancia de Windows

> **Note**
>
> Este tema se aplica únicamente a las instancias de Windows.

La instancia de Windows incluye un volumen de EBS que sirve como volumen raíz. Si la instancia de Windows utiliza controladores PV o Citrix PV de AWS, puede agregar opcionalmente hasta 25 volúmenes, con lo que se obtiene un total de 26 volúmenes. Para obtener más información, consulte Límites de volumen de instancias.

Según el tipo de instancia, tendrá de 0 a 24 volúmenes de almacén de instancias posibles disponibles para la instancia. Para utilizar cualquiera de los volúmenes de almacén de instancias disponibles para su instancia, debe especificarlos al crear su AMI o al iniciar la instancia. También puede añadir volúmenes de EBS al crear la AMI o al iniciar la instancia, o adjuntarlos mientras la instancia se está ejecutando.

Al añadir un volumen a la instancia, escriba el nombre del dispositivo que utiliza Amazon EC2. Para obtener más información, consulte Nombres de dispositivos en las instancias de Amazon EC2. AWS Las Imágenes de máquina de Amazon (AMI) de Windows contienen una serie de controladores utilizados por Amazon EC2 para asignar el almacén de instancias y los volúmenes de EBS a los discos y las letras de unidad de Windows. Si inicia una instancia desde una AMI de Windows que utiliza controladores PV o Citrix PV de AWS, puede utilizar las relaciones descritas en esta página para asignar los discos de Windows al almacén de instancias y los volúmenes de EBS. Si la AMI de Windows utiliza controladores Red Hat PV, puede actualizar la instancia para utilizar los controladores Citrix. Para obtener más información, consulte the section called “Actualizar controladores PV”.

Contenido

Listar volúmenes NVMe

Puede encontrar los discos de la instancia de Windows que utilizan Disk Management o PowerShell.

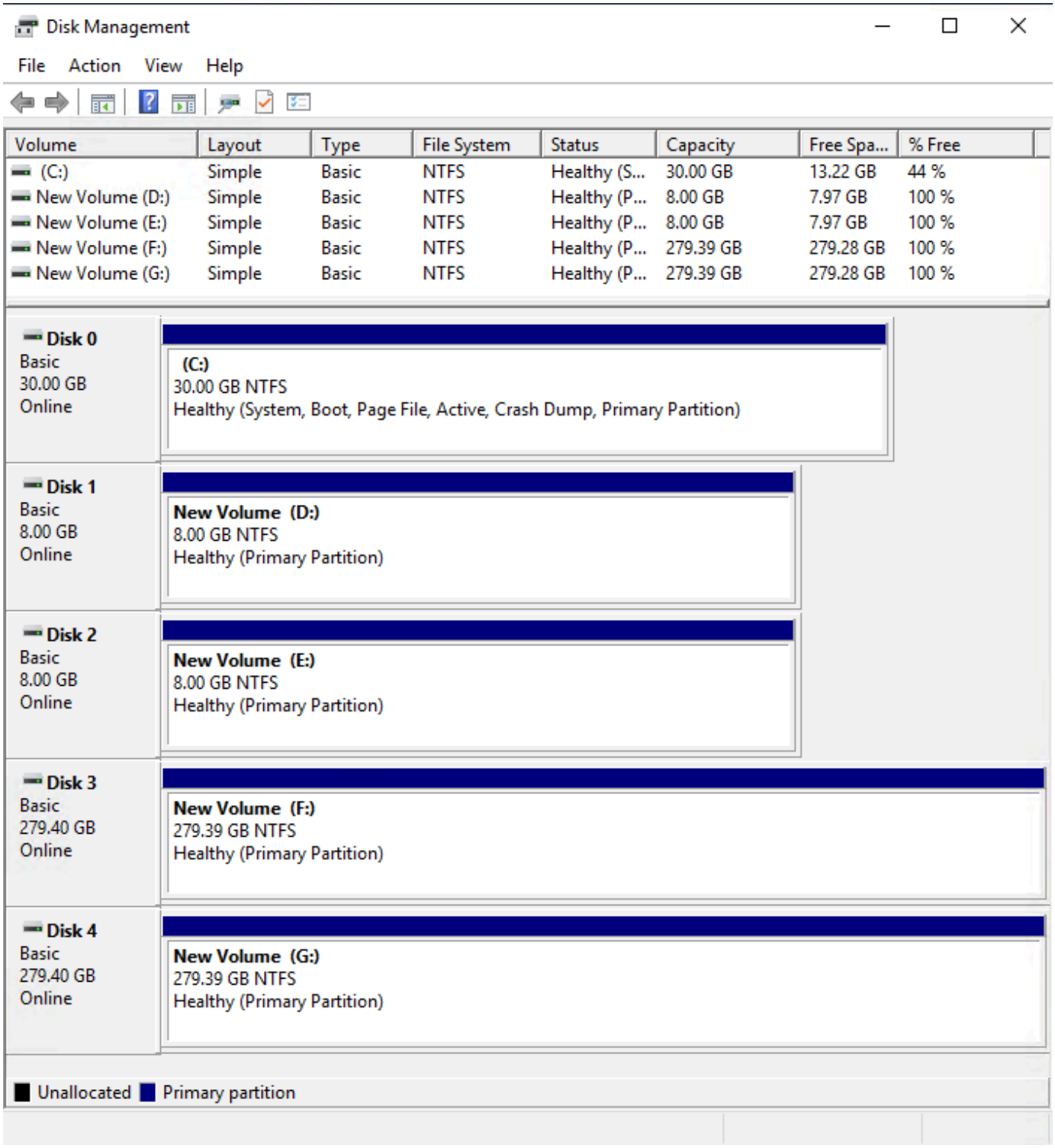
Listar discos NVMe utilizando Disk Management

Puede encontrar los discos de la instancia de Windows que utilizan Disk Management de Windows.

Para encontrar los discos en su instancia de Windows

1. Inicie sesión en la instancia de Windows mediante el Escritorio remoto. Para obtener más información, consulte Conexión con la instancia de Windows de.
2. Inicie la utilidad de Administración de discos.
3. Revise los discos. El volumen raíz es un volumen de EBS montado como `C:\`. Si no se muestran otros discos, no ha especificado volúmenes adicionales al crear la AMI o al iniciar la instancia.

   A continuación se muestra un ejemplo que muestra los discos que están disponibles si inicias una `r5d.4xlarge` instancia con dos volúmenes de EBS adicionales.


Disk Management
File Action View Help
Volume Layout Type File System Status Capacity Free Spa... % Free
(C:) Simple Basic NTFS Healthy (S... 30.00 GB 13.22 GB 44 %
New Volume (D:) Simple Basic NTFS Healthy (P... 8.00 GB 7.97 GB 100 %
New Volume (E:) Simple Basic NTFS Healthy (P... 8.00 GB 7.97 GB 100 %
New Volume (F:) Simple Basic NTFS Healthy (P... 279.39 GB 279.28 GB 100 %
New Volume (G:) Simple Basic NTFS Healthy (P... 279.39 GB 279.28 GB 100 %
Disk 0
Basic
30.00 GB
Online
(C:)
30.00 GB NTFS
Healthy (System, Boot, Page File, Active, Crash Dump, Primary Partition)
Disk 1
Basic
8.00 GB
Online
New Volume (D:)
8.00 GB NTFS
Healthy (Primary Partition)
Disk 2
Basic
8.00 GB
Online
New Volume (E:)
8.00 GB NTFS
Healthy (Primary Partition)
Disk 3
Basic
279.40 GB
Online
New Volume (F:)
279.39 GB NTFS
Healthy (Primary Partition)
Disk 4
Basic
279.40 GB
Online
New Volume (G:)
279.39 GB NTFS
Healthy (Primary Partition)
Unallocated
Primary partition

Listar discos NVMe utilizando PowerShell

El siguiente script de PowerShell enumera cada disco y el nombre y volumen de su dispositivo correspondiente. Está diseñado para su uso con instancias integradas en el AWS Nitro System, que utilizan volúmenes de EBS de NVMe y de almacén de instancias.

Conéctate a la instancia de Windows y ejecuta el siguiente comando para habilitar la ejecución de scripts de PowerShell.

```
Set-ExecutionPolicy RemoteSigned
```

Copia el siguiente script y guárdalo como `mapping.ps1` en la instancia de Windows.

```
# List the disks for NVMe volumes

function Get-EC2InstanceMetadata {
    param([string]$Path)
    (Invoke-WebRequest -Uri "http://169.254.169.254/latest/$Path").Content
}

function GetEBSVolumeId {
    param($Path)
    $SerialNumber = (Get-Disk -Path $Path).SerialNumber
    if($SerialNumber -clike 'vol*'){
        $EbsVolumeId = $SerialNumber.Substring(0,20).Replace("vol","vol-")
    }
    else {
       $EbsVolumeId = $SerialNumber.Substring(0,20).Replace("AWS","AWS-")
    }
    return $EbsVolumeId
}

function GetDeviceName{
    param($EbsVolumeId)
    if($EbsVolumeId -clike 'vol*'){

        $Device  = ((Get-EC2Volume -VolumeId $EbsVolumeId ).Attachment).Device
        $VolumeName = ""
    }
     else {
        $Device = "Ephemeral"
        $VolumeName = "Temporary Storage"
    }
```

```
    Return $Device,$VolumeName
}

function GetDriveLetter{
    param($Path)
    $DiskNumber =  (Get-Disk -Path $Path).Number
    if($DiskNumber -eq 0){
        $VirtualDevice = "root"
        $DriveLetter = "C"
        $PartitionNumber = (Get-Partition -DriveLetter C).PartitionNumber
    }
    else
    {
        $VirtualDevice = "N/A"
        $DriveLetter = (Get-Partition -DiskNumber $DiskNumber).DriveLetter
        if(!$DriveLetter)
        {
            $DriveLetter = ((Get-Partition -DiskId $Path).AccessPaths).Split(",")[0]
        }
        $PartitionNumber = (Get-Partition -DiskId $Path).PartitionNumber
    }

    return $DriveLetter,$VirtualDevice,$PartitionNumber

}

$Report = @()
foreach($Path in (Get-Disk).Path)
{
    $Disk_ID = ( Get-Partition -DiskId $Path).DiskId
    $Disk = ( Get-Disk -Path $Path).Number
    $EbsVolumeId  = GetEBSVolumeId($Path)
    $Size =(Get-Disk -Path $Path).Size
    $DriveLetter,$VirtualDevice, $Partition = (GetDriveLetter($Path))
    $Device,$VolumeName = GetDeviceName($EbsVolumeId)
    $Disk = New-Object PSObject -Property @{
      Disk          = $Disk
      Partitions    = $Partition
      DriveLetter   = $DriveLetter
      EbsVolumeId   = $EbsVolumeId
      Device        = $Device
      VirtualDevice = $VirtualDevice
      VolumeName= $VolumeName
    }
```

```
 $Report += $Disk
}

$Report | Sort-Object Disk | Format-Table -AutoSize -Property Disk, Partitions,
 DriveLetter, EbsVolumeId, Device, VirtualDevice, VolumeName
```

Ejecuta el script de la siguiente manera:

```
PS C:\> .\mapping.ps1
```

A continuación se muestra un ejemplo de salida para una instancia con un volumen raíz, dos volúmenes EBS y dos volúmenes de almacén de instancias.

```
Disk Partitions DriveLetter EbsVolumeId           Device    VirtualDevice VolumeName
---- ---------- ----------- -----------           ------    ------------- ----------
   0          1 C           vol-03683f1d861744bc7 /dev/sda1 root
   1          1 D           vol-082b07051043174b9 xvdb      N/A
   2          1 E           vol-0a4064b39e5f534a2 xvdc      N/A
   3          1 F           AWS-6AAD8C2AEEE1193F0 Ephemeral N/A           Temporary
 Storage
   4          1 G           AWS-13E7299C2BD031A28 Ephemeral N/A           Temporary
 Storage
```

Si no configuró sus credenciales para Herramientas de Windows PowerShell en la instancia de Windows, el script no puede obtener el ID del volumen de EBS y utilizará N/A en la columna `EbsVolumeId`.

Asignar volúmenes EBS de NVMe

Con las instancias integradas en el AWS Nitro System, los volúmenes de EBS se exponen como dispositivos NVMe. Utilice el comando Get-Disk para mapear números de discos de Windows a ID de volúmenes de EBS.

```
PS C:\> Get-Disk
Number Friendly Name Serial Number                    HealthStatus
 OperationalStatus      Total Size Partition

                     Style
------ ------------ -------------                    ------------
 -----------------      ---------- ----------
3      NVMe Amazo... AWS6AAD8C2AEEE1193F0_00000001.   Healthy              Online
             279.4 GB MBR
```

```
4      NVMe Amazo... AWS13E7299C2BD031A28_00000001.   Healthy            Online
             279.4 GB MBR
2      NVMe Amazo... vol0a4064b39e5f534a2_00000001.   Healthy            Online
               8 GB MBR
0      NVMe Amazo... vol03683f1d861744bc7_00000001.   Healthy            Online
              30 GB MBR
1      NVMe Amazo... vol082b07051043174b9_00000001.   Healthy            Online
               8 GB MBR
```

También puede ejecutar el comando ebsnvme-id para asignar números de disco NVMe a identificadores de volumen de EBS y nombres de dispositivos.

```
PS C:\> C:\PROGRAMDATA\Amazon\Tools\ebsnvme-id.exe
Disk Number: 0
Volume ID: vol-03683f1d861744bc7
Device Name: sda1

Disk Number: 1
Volume ID: vol-082b07051043174b9
Device Name: xvdb

Disk Number: 2
Volume ID: vol-0a4064b39e5f534a2
Device Name: xvdc
```

Listar volúmenes

Puede encontrar los discos de la instancia de Windows que utilizan Disk Management o PowerShell.

Listar discos utilizando Disk Management

Puede encontrar los discos de la instancia de Windows que utilizan Disk Management de Windows.

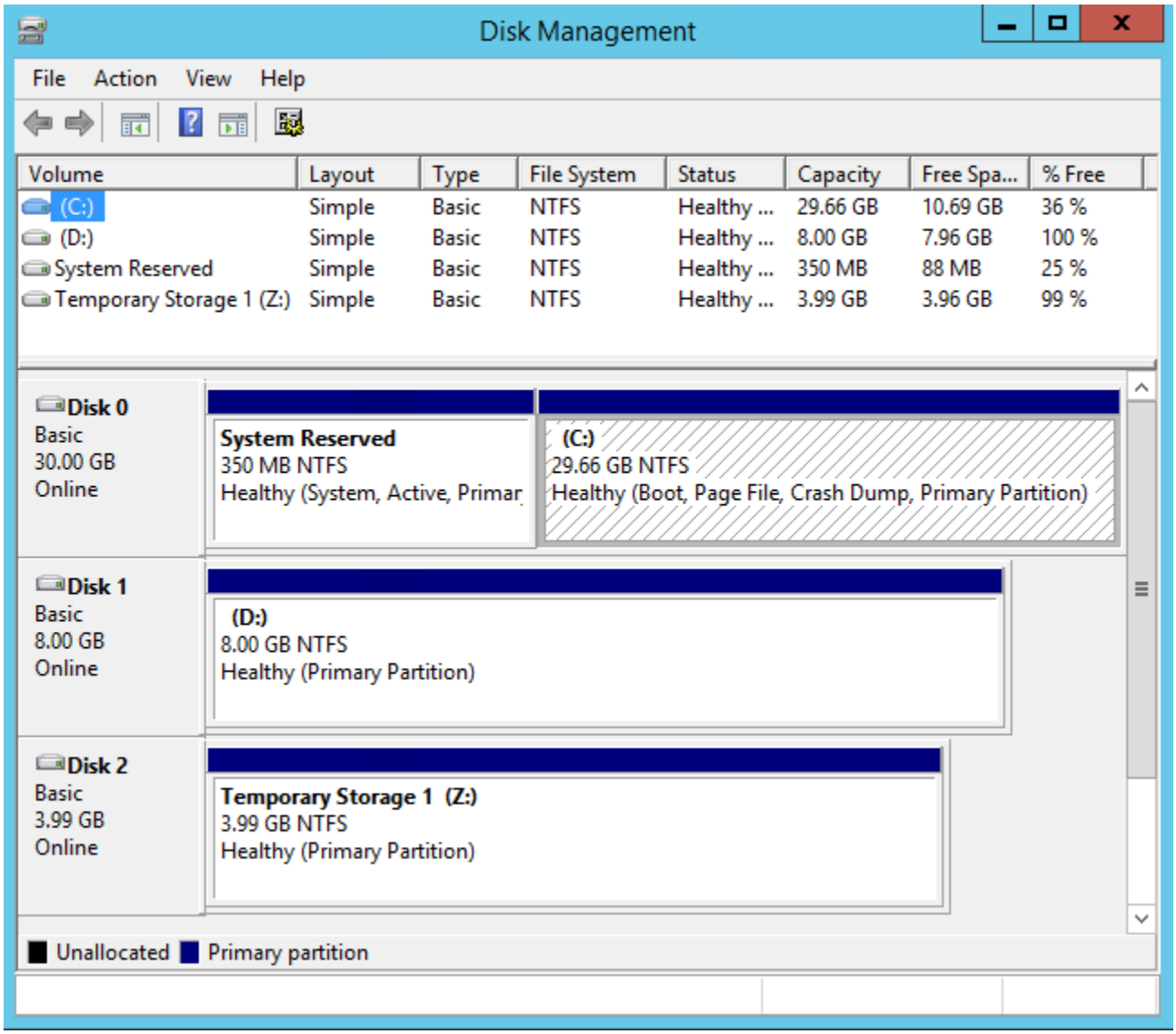
Para encontrar los discos en su instancia de Windows

1. Inicie sesión en la instancia de Windows mediante el Escritorio remoto. Para obtener más información, consulte Conexión con la instancia de Windows de.
2. Inicie la utilidad de Administración de discos.

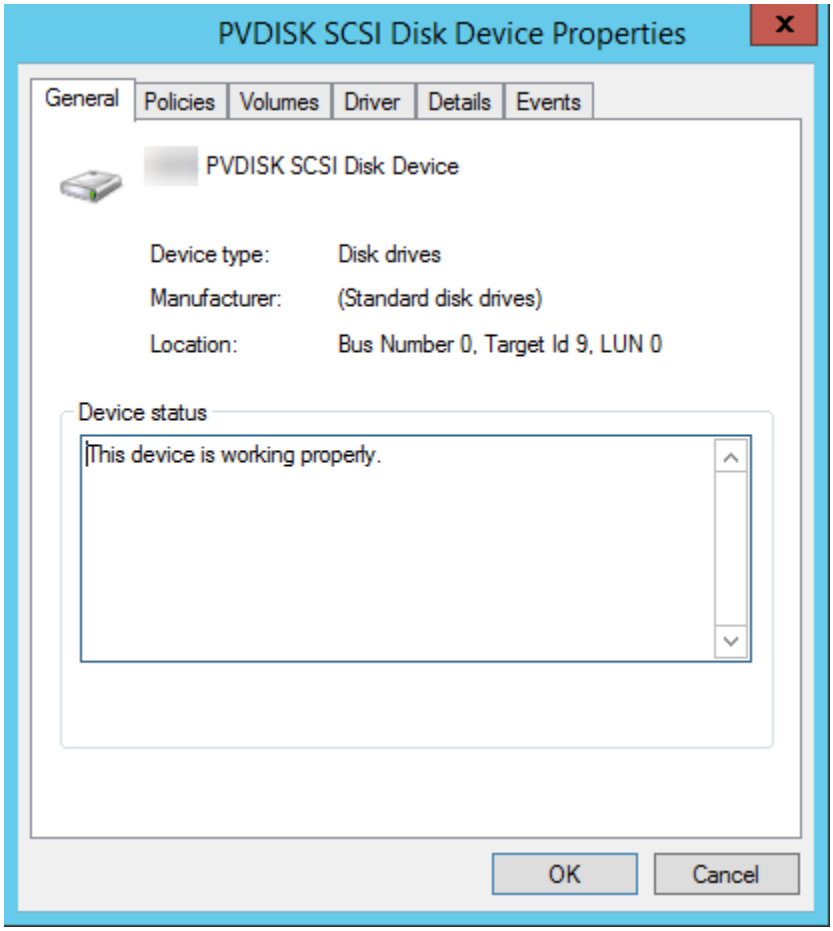
   En la barra de tareas, haga clic con el botón derecho en el logotipo de Windows y, a continuación, elija Administración de discos.

3. Revise los discos. El volumen raíz es un volumen de EBS montado como `C:\`. Si no se muestran otros discos, no ha especificado volúmenes adicionales al crear la AMI o al iniciar la instancia.

   A continuación se indica un ejemplo que muestra los discos disponibles si inicia una instancia `m3.medium` con un volumen de almacén de instancias (disco 2) y un volumen de EBS adicional (disco 1).



4. Haga clic con el botón derecho en el panel gris con la etiqueta Disco 1 y, a continuación, seleccione Propiedades. Anote el valor de Ubicación y búsquelo en las tablas en Asignar dispositivos de disco a nombres de dispositivos. Por ejemplo, el siguiente disco tiene la ubicación Bus Number 0, Target Id 9, LUN 0. Según la tabla de volúmenes de EBS, el nombre de dispositivo de esta ubicación es `xvdj`.



Asignar dispositivos de disco a nombres de dispositivos

El controlador del dispositivo de bloques de la instancia asigna los nombres reales de los volúmenes cuando se montan.

Mapeos

- Volúmenes de almacén de instancias
- Volúmenes de EBS

Volúmenes de almacén de instancias

La siguiente tabla describe cómo los controladores Citrix PV y PV de AWS asignan volúmenes de almacén de instancias de memoria rápida no volátil de baja latencia (NVMe) a volúmenes de Windows. El número de volúmenes de almacén de instancias disponibles se determina por el tipo de instancia. Para obtener más información, consulte Volúmenes de almacén de instancias.

Ubicación	Nombre del dispositivo
Bus Number 0, Target ID 78, LUN 0	xvdca
Bus Number 0, Target ID 79, LUN 0	xvdcb
Bus Number 0, Target ID 80, LUN 0	xvdcc
Bus Number 0, Target ID 81, LUN 0	xvdcd
Bus Number 0, Target ID 82, LUN 0	xvdce
Bus Number 0, Target ID 83, LUN 0	xvdcf
Bus Number 0, Target ID 84, LUN 0	xvdcg
Bus Number 0, Target ID 85, LUN 0	xvdch
Bus Number 0, Target ID 86, LUN 0	xvdci
Bus Number 0, Target ID 87, LUN 0	xvdcj
Bus Number 0, Target ID 88, LUN 0	xvdck
Bus Number 0, Target ID 89, LUN 0	xvdcl

Volúmenes de EBS

La siguiente tabla describe cómo los controladores Citrix PV y PV de AWS asignan volúmenes de EBS que no son NVMe a volúmenes de Windows.

Ubicación	Nombre del dispositivo
Bus Number 0, Target ID 0, LUN 0	/dev/sda1
Bus Number 0, Target ID 1, LUN 0	xvdb
Bus Number 0, Target ID 2, LUN 0	xvdc
Bus Number 0, Target ID 3, LUN 0	xvdd

Ubicación	Nombre del dispositivo
Bus Number 0, Target ID 4, LUN 0	xvde
Bus Number 0, Target ID 5, LUN 0	xvdf
Bus Number 0, Target ID 6, LUN 0	xvdg
Bus Number 0, Target ID 7, LUN 0	xvdh
Bus Number 0, Target ID 8, LUN 0	xvdi
Bus Number 0, Target ID 9, LUN 0	xvdj
Bus Number 0, Target ID 10, LUN 0	xvdk
Bus Number 0, Target ID 11, LUN 0	xvdl
Bus Number 0, Target ID 12, LUN 0	xvdm
Bus Number 0, Target ID 13, LUN 0	xvdn
Bus Number 0, Target ID 14, LUN 0	xvdo
Bus Number 0, Target ID 15, LUN 0	xvdp
Bus Number 0, Target ID 16, LUN 0	xvdq
Bus Number 0, Target ID 17, LUN 0	xvdr
Bus Number 0, Target ID 18, LUN 0	xvds
Bus Number 0, Target ID 19, LUN 0	xvdt
Bus Number 0, Target ID 20, LUN 0	xvdu
Bus Number 0, Target ID 21, LUN 0	xvdv
Bus Number 0, Target ID 22, LUN 0	xvdw
Bus Number 0, Target ID 23, LUN 0	xvdx

Ubicación	Nombre del dispositivo
Bus Number 0, Target ID 24, LUN 0	xvdy
Bus Number 0, Target ID 25, LUN 0	xvdz

Listar discos utilizando PowerShell

El siguiente script de PowerShell enumera cada disco y el nombre y volumen de su dispositivo correspondiente.

Requisitos y limitaciones

- Requiere Windows Server 2012 o posterior.
- Requiere credenciales para obtener el ID de volumen de EBS. Puede configurar un perfil utilizando Tools for PowerShell o adjuntar una función de IAM a la instancia.
- No admite volúmenes NVMe.
- No admite discos dinámicos.

Conéctate a la instancia de Windows y ejecuta el siguiente comando para habilitar la ejecución de scripts de PowerShell.

```
Set-ExecutionPolicy RemoteSigned
```

Copia el siguiente script y guárdalo como `mapping.ps1` en la instancia de Windows.

```
# List the disks
function Convert-SCSITargetIdToDeviceName {
  param([int]$SCSITargetId)
  If ($SCSITargetId -eq 0) {
    return "sda1"
  }
  $deviceName = "xvd"
  If ($SCSITargetId -gt 25) {
    $deviceName += [char](0x60 + [int]($SCSITargetId / 26))
  }
  $deviceName += [char](0x61 + $SCSITargetId % 26)
  return $deviceName
}
```

```
[string[]]$array1 = @()
[string[]]$array2 = @()
[string[]]$array3 = @()
[string[]]$array4 = @()

Get-WmiObject Win32_Volume | Select-Object Name, DeviceID | ForEach-Object {
  $array1 += $_.Name
  $array2 += $_.DeviceID
}

$i = 0
While ($i -ne ($array2.Count)) {
  $array3 += ((Get-Volume -Path $array2[$i] | Get-Partition | Get-Disk).SerialNumber) -
replace "_[^ ]*$" -replace "vol", "vol-"
  $array4 += ((Get-Volume -Path $array2[$i] | Get-Partition | Get-Disk).FriendlyName)
  $i ++
}

[array[]]$array = $array1, $array2, $array3, $array4

Try {
  $InstanceId = Get-EC2InstanceMetadata -Category "InstanceId"
  $Region = Get-EC2InstanceMetadata -Category "Region" | Select-Object -ExpandProperty
 SystemName
}
Catch {
  Write-Host "Could not access the instance Metadata using AWS Get-EC2InstanceMetadata
 CMDLet.
Verify you have AWSPowershell SDK version '3.1.73.0' or greater installed and Metadata
 is enabled for this instance." -ForegroundColor Yellow
}
Try {
  $BlockDeviceMappings = (Get-EC2Instance -Region $Region -Instance
 $InstanceId).Instances.BlockDeviceMappings
  $VirtualDeviceMap = (Get-EC2InstanceMetadata -Category
 "BlockDeviceMapping").GetEnumerator() | Where-Object { $_.Key -ne "ami" }
}
Catch {
  Write-Host "Could not access the AWS API, therefore, VolumeId is not available.
Verify that you provided your access keys or assigned an IAM role with adequate
 permissions." -ForegroundColor Yellow
}
```

```
Get-disk | ForEach-Object {
  $DriveLetter = $null
  $VolumeName = $null
  $VirtualDevice = $null
  $DeviceName = $_.FriendlyName

  $DiskDrive = $_
  $Disk = $_.Number
  $Partitions = $_.NumberOfPartitions
  $EbsVolumeID = $_.SerialNumber -replace "_[^ ]*$" -replace "vol", "vol-"
  if ($Partitions -ge 1) {
    $PartitionsData = Get-Partition -DiskId $_.Path
    $DriveLetter = $PartitionsData.DriveLetter | Where-object { $_ -notin @("",
 $null) }
    $VolumeName = (Get-PSDrive | Where-Object { $_.Name -in
 @($DriveLetter) }).Description | Where-object { $_ -notin @("", $null) }
  }
  If ($DiskDrive.path -like "*PROD_PVDISK*") {
    $BlockDeviceName = Convert-SCSITargetIdToDeviceName((Get-WmiObject -Class
 Win32_Diskdrive | Where-Object { $_.DeviceID -eq ("\\.\PHYSICALDRIVE" +
 $DiskDrive.Number) }).SCSITargetId)
    $BlockDeviceName = "/dev/" + $BlockDeviceName
    $BlockDevice = $BlockDeviceMappings | Where-Object { $BlockDeviceName -like "*" +
 $_.DeviceName + "*" }
    $EbsVolumeID = $BlockDevice.Ebs.VolumeId
    $VirtualDevice = ($VirtualDeviceMap.GetEnumerator() | Where-Object { $_.Value -eq
 $BlockDeviceName }).Key | Select-Object -First 1
  }
  ElseIf ($DiskDrive.path -like "*PROD_AMAZON_EC2_NVME*") {
    $BlockDeviceName = (Get-EC2InstanceMetadata -Category
 "BlockDeviceMapping").ephemeral((Get-WmiObject -Class Win32_Diskdrive | Where-Object
 { $_.DeviceID -eq ("\\.\PHYSICALDRIVE" + $DiskDrive.Number) }).SCSIPort - 2)
    $BlockDevice = $null
    $VirtualDevice = ($VirtualDeviceMap.GetEnumerator() | Where-Object { $_.Value -eq
 $BlockDeviceName }).Key | Select-Object -First 1
  }
  ElseIf ($DiskDrive.path -like "*PROD_AMAZON*") {
    if ($DriveLetter -match '[^a-zA-Z0-9]') {
      $i = 0
      While ($i -ne ($array3.Count)) {
        if ($array[2][$i] -eq $EbsVolumeID) {
          $DriveLetter = $array[0][$i]
          $DeviceName = $array[3][$i]
        }
```

```
        $i ++
      }
    }
    $BlockDevice = ""
    $BlockDeviceName = ($BlockDeviceMappings | Where-Object { $_.ebs.VolumeId -eq
 $EbsVolumeID }).DeviceName
   }
   ElseIf ($DiskDrive.path -like "*NETAPP*") {
    if ($DriveLetter -match '[^a-zA-Z0-9]') {
      $i = 0
      While ($i -ne ($array3.Count)) {
        if ($array[2][$i] -eq $EbsVolumeID) {
          $DriveLetter = $array[0][$i]
          $DeviceName = $array[3][$i]
        }
        $i ++
      }
    }
    $EbsVolumeID = "FSxN Volume"
    $BlockDevice = ""
    $BlockDeviceName = ($BlockDeviceMappings | Where-Object { $_.ebs.VolumeId -eq
 $EbsVolumeID }).DeviceName
   }
   Else {
    $BlockDeviceName = $null
    $BlockDevice = $null
   }
   New-Object PSObject -Property @{
    Disk          = $Disk;
    Partitions    = $Partitions;
    DriveLetter   = If ($DriveLetter -eq $null) { "N/A" } Else { $DriveLetter };
    EbsVolumeId   = If ($EbsVolumeID -eq $null) { "N/A" } Else { $EbsVolumeID };
    Device        = If ($BlockDeviceName -eq $null) { "N/A" } Else
 { $BlockDeviceName };
    VirtualDevice = If ($VirtualDevice -eq $null) { "N/A" } Else { $VirtualDevice };
    VolumeName    = If ($VolumeName -eq $null) { "N/A" } Else { $VolumeName };
    DeviceName    = If ($DeviceName -eq $null) { "N/A" } Else { $DeviceName };
   }
} | Sort-Object Disk | Format-Table -AutoSize -Property Disk, Partitions, DriveLetter,
 EbsVolumeId, Device, VirtualDevice, DeviceName, VolumeName
```

Ejecuta el script de la siguiente manera:

```
PS C:\> .\mapping.ps1
```

A continuación, se muestra un ejemplo del resultado.

```
Disk  Partitions  DriveLetter   EbsVolumeId             Device      VirtualDevice
 DeviceName              VolumeName
----  ----------  -----------   -----------             ------      -------------
 ----------              ----------
   0           1            C   vol-0561f1783298efedd   /dev/sda1   N/A
 NVMe Amazon Elastic B   N/A
   1           1            D   vol-002a9488504c5e35a   xvdb        N/A
 NVMe Amazon Elastic B   N/A
   2           1            E   vol-0de9d46fcc907925d   xvdc        N/A
 NVMe Amazon Elastic B   N/A
```

Si no proporcionaste tus credenciales en la instancia de Windows, el script no puede obtener el ID del volumen de EBS y utilizará N/A en la columna `EbsVolumeId`.

Instantáneas de Amazon EBS basadas en VSS de Windows consistentes con la aplicación

> **Note**
>
> Las instantáneas coherentes con la aplicación basadas en VSS de Windows solo son compatibles con las instancias de Windows.

Puede tomar instantáneas coherentes con la aplicación de todos los volúmenes de Amazon EBS que se hayan adjuntado a las instancias de Windows de Amazon EC2 con AWS Systems Manager Run Command. El proceso de instantáneas usa el servicio Volume Shadow Copy Service (VSS) de Windows para crear copias de seguridad de nivel de volumen de EBS de aplicaciones con reconocimiento de VSS. Las instantáneas incluyen datos de transacciones pendientes entre estas aplicaciones y el disco. No es necesario que apague sus instancias o las desconecte cuando necesite realizar una copia de seguridad todos los volúmenes adjuntos.

Las instantáneas de EBS basadas en VSS no incurren en ningún costo adicional. Solo pagará por las instantáneas de EBS creadas por el proceso de copia de seguridad. Para obtener más información, consulte ¿Cómo se facturan las instantáneas EBS de Amazon EBS?

Contenido

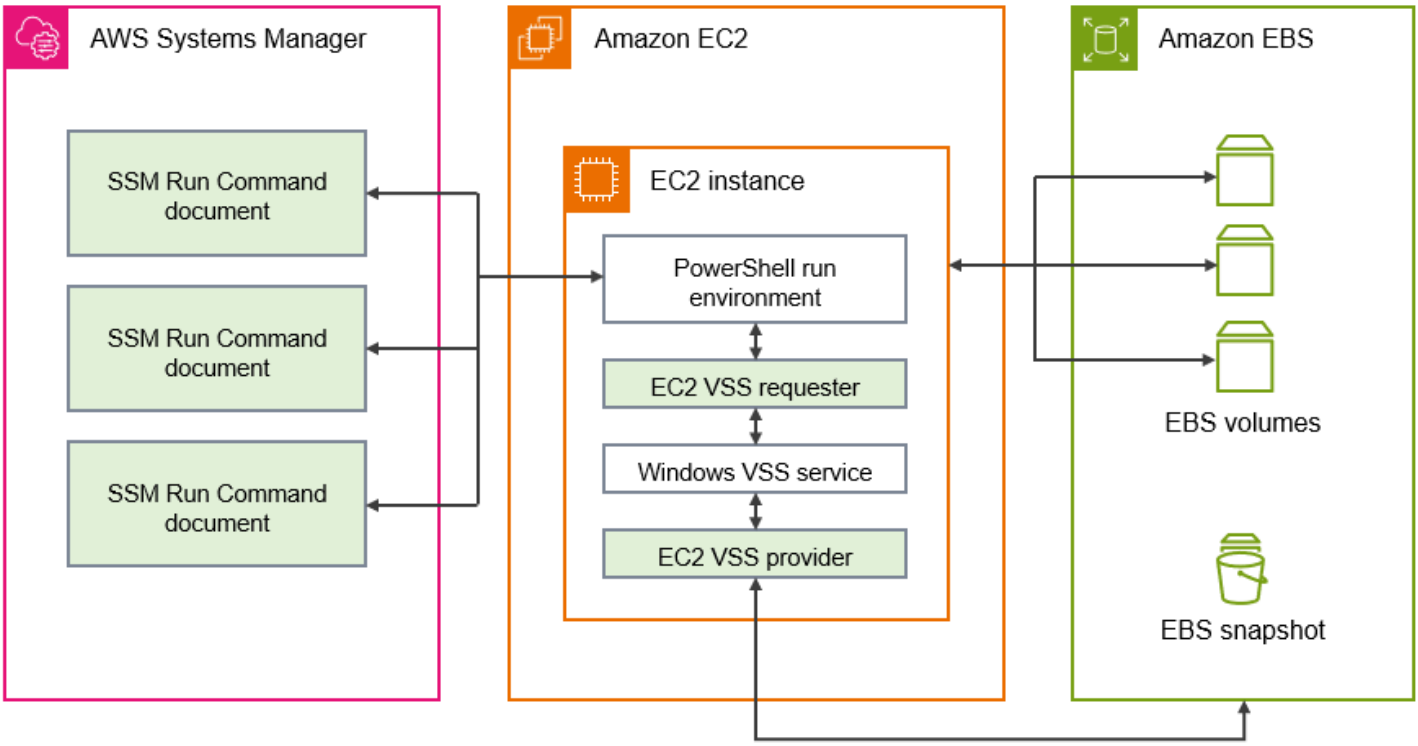
¿Qué es VSS?

Volume Snapshot Copy Service (VSS) es una tecnología de copia de seguridad y recuperación que está incluida en Microsoft Windows. Puede crear copias de seguridad, o instantáneas, de archivos o volúmenes del ordenador mientras están en uso. Para obtener más información, consulte Volume Shadow Copy Service.

Para crear una instantánea coherente con la aplicación, se utilizan los siguientes componentes de software.

- Servicio VSS: parte del sistema operativo Windows.
- Solicitante de VSS: el software que solicita la creación de instantáneas.
- Escritor de VSS: normalmente se proporciona como parte de una aplicación, como SQL Server, para garantizar que un conjunto de datos sea coherente para poder hacer copias de seguridad.
- Proveedor de VSS: el componente que crea las instantáneas de los volúmenes subyacentes.

La solución de instantáneas de Amazon EBS basadas en VSS de Windows consta de varios documentos de Systems Manager (SSM) Run Command que facilitan la creación de copias de seguridad y un paquete del distribuidor de Systems Manager denominado `AwsVssComponents`, el cual incluye un solicitante de VSS de EC2 y un proveedor de VSS de EC2. El paquete `AwsVssComponents` debe estar instalado en instancias de Amazon EC2 para obtener instantáneas de volúmenes de EBS coherentes con las aplicaciones. En el siguiente diagrama se muestra la relación entre estos componentes de software.



Cómo funciona la solución de instantáneas Amazon EBS basada en VSS

El proceso de tomar scripts de instantáneas de EBS basadas en VSS y coherentes con la aplicación consta de los siguientes pasos.

1. Complete el Requisitos previos.
2. Ingrese los parámetros para el documento de SSM `AWSEC2-VssInstallAndSnapshot` y ejecute este documento mediante Run Command. Para obtener más información, consulte Ejecute el documento de comandos AWSEC2-VssInstallAndSnapshot (recomendado).
3. El servicio VSS de Windows de la instancia coordina todas las operaciones de E/S en curso para las aplicaciones en ejecución.
4. El sistema vacía todos los búferes de E/S y detiene temporalmente todas las operaciones de E/S. La pausa dura, como máximo, diez segundos.
5. Durante la pausa, el sistema crea instantáneas de todos los volúmenes asociados a la instancia.
6. La pausa se levanta y E/S reanuda la operación.
7. El sistema añade todas las instantáneas recién creadas a la lista de instantáneas de EBS. El sistema etiqueta todas las instantáneas de EBS compatibles con VSS creadas correctamente por este proceso con AppConsistent:true.

8. Si tiene que restaurar datos a partir de una instantánea, puede usar el proceso de EBS estándar de crear un volumen a partir de una instantánea, o bien puede restaurar todos los volúmenes en una instancia mediante un script de muestra, como se describe en Restauración de volúmenes de EBS desde instantáneas de EBS compatibles con VSS.

Requisitos previos

Puede crear instantáneas de VSS basadas en EBS con Systems Manager Run Command, AWS Backup o Amazon Data Lifecycle Manager. Los siguientes requisitos previos se aplican a todas las soluciones.

Requisitos previos

- Requisitos del sistema
- Permisos de IAM
- Componentes de VSS

Requisitos del sistema

Instalar el agente de Systems Manager

AWS Systems Manager (Systems Manager) orquesta VSS mediante PowerShell. Asegúrese de haber instalado la versión `3.0.502.0` o una posterior de SSM Agent en su instancia de Amazon EC2. Si ya usa una versión anterior de SSM Agent, actualícela mediante Run Command. Para obtener más información, consulte Configuración de Systems Manager para instancias de Amazon EC2 y Uso de SSM Agent en instancias de Amazon EC2 para Windows Server en la Guía del usuario de AWS Systems Manager.

Requisitos de instancia de Windows Amazon EC2

Las instantáneas de EBS basadas en VSS son compatibles con las instancias que ejecutan Windows Server 2012 y versiones posteriores. Para obtener información sobre las versiones anteriores de Windows, consulte la tabla de compatibilidad de versiones de Windows en Historial de versiones de la solución AWS VSS.

Versión de .NET Framework

El paquete `AwsVssComponents` requiere la versión `4.6` o una posterior de .NET Framework. Las versiones del sistema operativo Windows anteriores a Windows Server 2016 utilizan de forma

predeterminada una versión anterior de .NET Framework. Si la instancia usa una versión anterior de .NET Framework, debe instalar la versión `4.6` o posterior mediante Windows Update.

Versión de AWS Tools for Windows PowerShell

Asegúrese de que la instancia esté ejecutando la versión `3.3.48.0` o una posterior de AWS Tools for Windows PowerShell. Para comprobar qué versión tiene, ejecute el siguiente comando en la instancia en el terminal de PowerShell.

```
C:\> Get-AWSPowerShellVersion
```

Si necesita actualizar AWS Tools for Windows PowerShell en su instancia, consulte Instalación de AWS Tools for Windows PowerShell en la Guía del usuario de AWS Tools for Windows PowerShell.

Versión de Windows Powershell

Asegúrese de que la instancia esté ejecutando la versión principal de Windows PowerShell `3`, `4` o `5`. Para comprobar qué versión tiene, ejecute el siguiente comando en la instancia en un terminal de PowerShell.

```
C:\> $PSVersionTable.PSVersion
```

Modo de lenguaje de PowerShell

Asegúrese de que la instancia tenga el modo de lenguaje de PowerShell configurado en `FullLanguage`. Para obtener más información, consulte about_Language_Modes en la documentación de Microsoft.

Permisos de IAM

El rol de IAM asociado a su instancia de Windows de Amazon EC2 debe tener permiso para crear instantáneas coherentes con la aplicación con VSS. Para conceder los permisos necesarios, puede asociar la política `AWSEC2VssSnapshotPolicy` a su perfil de instancia.

A través de la política se le permite a Systems Manager realizar las siguientes acciones:

- Crear y etiquetar instantáneas de EBS
- Crear y etiquetar imágenes de máquina de Amazon (AMI)

- Adjuntar metadatos, como el ID del dispositivo, a las etiquetas de instantáneas predeterminadas que crea VSS.

Temas

Adjuntar la política de instantáneas habilitada para VSS a su perfil de instancia

Para conceder permisos para las instantáneas habilitadas para VSS para su instancia, debe adjuntar la política administrada AWSEC2VssSnapshotPolicy a la función de perfil de instancia de la siguiente manera. Es importante que se asegure de que su instancia cumpla con todos los Requisitos del sistema.

> **Note**
>
> Para usar la política administrada, la instancia debe tener instalada la versión del paquete `AwsVssComponents 2.3.1` o posterior. Para ver el historial de versiones, consulte Versiones del paquete AwsVssComponents.
> Si tiene una versión anterior del paquete `AwsVssComponents` instalada en la instancia, consulte Política heredada.

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, seleccione Roles para ver una lista de los roles de IAM a los que tiene acceso.
3. Seleccione el enlace del nombre del rol para el rol asociado a la instancia. Se abre la página de detalle del rol.
4. Para adjuntar la política administrada, seleccione Añadir permisos, que se encuentra en la esquina superior derecha del panel de lista. Luego, seleccione Adjuntar políticas en la lista desplegable.
5. Para optimizar los resultados, escriba el nombre de la política en la barra de búsqueda (`AWSEC2VssSnapshotPolicy`).

6. Seleccione la casilla situada junto al nombre de la política que desea adjuntar y elija Añadir permisos.

Política administrada para crear instantáneas de VSS

Una política administrada de AWS es una política independiente que Amazon proporciona a los clientes de AWS. Las políticas administradas de AWS están diseñadas para conceder permisos para casos de uso comunes. No se pueden cambiar los permisos definidos en las políticas administradas de AWS. Sin embargo, puede copiar la política y utilizarla como base para una política administrada por el cliente que sea específica para su caso de uso.

Para obtener más información acerca de las políticas administradas de AWS, consulte Políticas administradas de AWS en la Guía del usuario de IAM.

Para usar la política AWSEC2VssSnapshotPolicy, la política administrada, puede asociarla al rol de IAM asociado a sus instancias de EC2 de Windows. Esta política permite a la solución VSS de EC2 crear y añadir etiquetas a las imágenes de máquina de Amazon (AMI) y a las instantáneas de EBS. Para adjuntar la política, consulte Adjuntar la política de instantáneas habilitada para VSS a su perfil de instancia.

Permisos concedidos por AWSEC2VssSnapshotPolicy

La política AWSEC2VssSnapshotPolicy incluye los siguientes permisos de Amazon EC2:

- ec2:CreateTags: agregue etiquetas a las instantáneas y AMI de EBS para ayudar a identificar y clasificar los recursos.
- ec2:DescribeInstanceAttribute: recupere los volúmenes de EBS y las asignaciones de dispositivos de bloques correspondientes que están adjuntos a la instancia de destino.
- ec2:CreateSnapshots: cree instantáneas de volúmenes de EBS.
- ec2:CreateImage: cree una AMI a partir de una instancia de EC2 en ejecución.
- ec2:DescribeImages: recupere la información de las AMI e instantáneas de EC2.
- EC2:DescribeSnapshots: determine la hora y el estado de las instantáneas para comprobar la coherencia de la aplicación.

Ejemplo de políticas

A continuación, se muestra un ejemplo de la política AWSEC2VssSnapshotPolicy.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DescribeInstanceInfo",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstanceAttribute"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:SourceInstanceARN": "*${ec2:InstanceId}"
                }
            }
        },
        {
            "Sid": "CreateSnapshotsWithTag",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSnapshots"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:snapshot/*"
            ],
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/AwsVssConfig": "*"
                }
            }
        },
        {
            "Sid": "CreateSnapshotsAccessInstance",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSnapshots"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Condition": {
```

```
                "StringLike": {
                    "ec2:SourceInstanceARN": "*${ec2:InstanceId}"
                }
            }
        },
        {
            "Sid": "CreateSnapshotsAccessVolume",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSnapshots"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:volume/*"
            ]
        },
        {
            "Sid": "CreateImageWithTag",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateImage"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:snapshot/*",
                "arn:aws:ec2:*:*:image/*"
            ],
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/AwsVssConfig": "*"
                }
            }
        },
        {
            "Sid": "CreateImageAccessInstance",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateImage"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:SourceInstanceARN": "*${ec2:InstanceId}"
                }
```

```
            }
        },
        {
            "Sid": "CreateTagsOnResourceCreation",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": [
                "arn:aws:ec2:*:*:snapshot/*",
                "arn:aws:ec2:*:*:image/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": [
                        "CreateImage",
                        "CreateSnapshots"
                    ]
                }
            }
        },
        {
            "Sid": "CreateTagsAfterResourceCreation",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": [
                "arn:aws:ec2:*:*:snapshot/*",
                "arn:aws:ec2:*:*:image/*"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/AwsVssConfig": "*"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "AppConsistent",
                        "Device"
                    ]
                }
            }
        },
        {
            "Sid": "DescribeImagesAndSnapshots",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeImages",
```

```
                "ec2:DescribeSnapshots"
            ],
            "Resource": "*"
        }
    ]
}
```

Optimización de los permisos para casos de uso específicos (avanzado)

La política administrada `AWSEC2VssSnapshotPolicy` incluye permisos para todas las formas en que puede crear instantáneas compatibles con VSS. Puede crear una política personalizada que incluya solo los permisos que necesite.

Caso de uso: crear AMI, Caso de uso: usar servicio de AWS Backup

Si utiliza exclusivamente la opción `CreateAmi` o si crea instantáneas compatibles con VSS únicamente a través del servicio de AWS Backup, puede simplificar las instrucciones de política de la siguiente manera.

- Omita las instrucciones de política identificadas por los siguientes ID de instrucción (SID):
  - `CreateSnapshotsWithTag`
  - `CreateSnapshotsAccessInstance`
  - `CreateSnapshotsAccessVolume`
- Ajuste la instrucción `CreateTagsOnResourceCreation` de la siguiente manera:
  - Elimine `arn:aws:ec2:*:*:snapshot/*` del recurso.
  - Elimine `CreateSnapshots` de la `ec2:CreateAction` condición.
- Ajuste la instrucción `CreateTagsAfterResourceCreation` para eliminar `arn:aws:ec2:*:*:snapshot/*` de los recursos.
- Ajuste la instrucción `DescribeImagesAndSnapshots` para eliminar `ec2:DescribeSnapshots` de la acción de la instrucción.

Caso de uso: solo instantánea

Si no utiliza la opción `CreateAmi`, puede simplificar las instrucciones de política de la siguiente manera.

- Omita las declaraciones de política identificadas por los siguientes ID de instrucción (SID):
  - `CreateImageAccessInstance`

  - `CreateImageWithTag`
- Ajuste la instrucción `CreateTagsOnResourceCreation` de la siguiente manera:
  - Elimine `arn:aws:ec2:*:*:image/*` del recurso.
  - Elimine `CreateImage` de la `ec2:CreateAction` condición.
- Ajuste la instrucción `CreateTagsAfterResourceCreation` para eliminar `arn:aws:ec2:*:*:image/*` de los recursos.
- Ajuste la instrucción `DescribeImagesAndSnapshots` para eliminar `ec2:DescribeImages` de la acción de la instrucción.

> **Note**
>
> Para garantizar que su política personalizada funcione como se espera, le recomendamos que revise e incorpore actualizaciones periódicas a la política administrada.

Política heredada (ya no se admite)

La política heredada que concede permisos para las instantáneas compatibles con VSS incluye los permisos de IAM que se recomendaban antes del lanzamiento de la política administrada `AWSEC2VssSnapshotPolicy`.

Si configuró un rol de instancia con la política anterior, puede seguir utilizándolo. Sin embargo, para garantizar que su política se mantiene actualizada con las últimas mejores prácticas de IAM y que alcanza las instrucciones de política en consecuencia, le recomendamos que sustituya la política heredada por la política administrada `AWSEC2VssSnapshotPolicy`.

Ejemplo de políticas

El siguiente ejemplo de política utiliza el `ec2:DescribeInstanceAttribute` que se admite en las versiones del paquete `AwsVssComponents` 2.2.1 y posteriores. Si tiene instalada una versión anterior del paquete `AwsVssComponents`, debe reemplazarla con la acción `ec2:DescribeInstances`.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
```

```
    "Effect": "Allow",
    "Action": "ec2:CreateTags",
    "Resource": [
     "arn:aws:ec2:*::snapshot/*",
     "arn:aws:ec2:*::image/*"
    ]
   },
   {
    "Effect": "Allow",
    "Action": [
     "ec2:DescribeInstanceAttribute",
     "ec2:CreateSnapshot",
     "ec2:CreateSnapshots",
     "ec2:CreateImage",
     "ec2:DescribeImages",
     "ec2:DescribeSnapshots"
    ],
    "Resource": "*"
   }
  ]
}
```

Para obtener más información sobre las políticas administradas de IAM, consulte las políticas administradas de AWS en la Guía del usuario de IAM.

Componentes de VSS

Para crear instantáneas coherentes con las aplicaciones en los sistemas operativos Windows, el paquete `AwsVssComponents` debe estar instalado en la instancia. El paquete contiene un agente de VSS de EC2 en la instancia que funciona como solicitante de VSS y un proveedor de VSS de EC2 para los volúmenes de EBS.

Existen varias formas de instalar el componente en una instancia existente:

- (Recomendado) Ejecute el documento de comandos AWSEC2-VssInstallAndSnapshot (recomendado). Se instala o actualiza automáticamente, si es necesario, cada vez que se ejecuta.
- Instalación manual de los componentes de VSS en una instancia.
- Actualización de los componentes de VSS en sus instancias en función de una programación.

También puede crear una AMI con el Generador de imágenes de EC2 que use el componente administrado por `aws-vss-components-windows` a fin de instalar el paquete

`AwsVssComponents` para la imagen. El componente administrado usa el Distribuidor de AWS Systems Manager para instalar el paquete. Una vez que el Generador de imágenes cree la imagen, todas las instancias que lance desde la AMI asociada tendrán el paquete VSS instalado. Para obtener más información sobre cómo crear una AMI con el paquete VSS instalado, consulte Componentes administrados mediante paquetes del Distribuidor para Windows en la Guía del usuario del Generador de imágenes de EC2.

Contenido

Instalación manual de los componentes de VSS en una instancia

Su instancia de EC2 de Windows debe tener componentes VSS instalados antes de poder crear instantáneas coherentes con las aplicaciones con Systems Manager. Si no ejecuta el documento de comandos `AWSEC2-VssInstallAndSnapshot` para instalar o actualizar automáticamente el paquete cada vez que crea instantáneas coherentes con las aplicaciones, debe instalar el paquete manualmente.

También debe realizar la instalación manualmente si piensa usar uno de los siguientes métodos para crear instantáneas coherentes con las aplicaciones a partir de su instancia de EC2.

- Creación de instantáneas de VSS mediante AWS Backup
- Creación de instantáneas de VSS con Amazon Data Lifecycle Manager

Si necesita realizar una instalación manual, le recomendamos que instale el paquete de componentes de AWS VSS más reciente para mejorar la fiabilidad y el rendimiento de las instantáneas coherentes con las aplicaciones en las instancias de EC2 de Windows.

> **Note**
>
> Para instalar o actualizar automáticamente el paquete `AwsVssComponents` cada vez que cree instantáneas coherentes con las aplicaciones, le recomendamos que utilice Systems Manager para ejecutar el documento `AWSEC2-VssInstallAndSnapshot`. Para obtener más información, consulte Ejecute el documento de comandos AWSEC2-VssInstallAndSnapshot (recomendado).

Para instalar los componentes de VSS en una instancia de Windows de Amazon EC2, siga los pasos de su entorno de preferencia.

Console

Para instalar los componentes de VSS mediante el Distribuidor de SSM

1. Abra la consola de AWS Systems Manager en https://console.aws.amazon.com/systems-manager/.
2. En el panel de navegación, elija Ejecutar comando.
3. Elija Run command (Ejecutar comando).
4. En Documento de comando, seleccione el botón situado junto a AWS-ConfigureAWSPackage.
5. En Parámetros de comando haga lo siguiente:
   a. Compruebe que Acción está establecido en Instalar.
   b. En Nombre, escriba `AwsVssComponents`.
   c. En Versión, escriba una versión o deje el campo vacío para que Systems Manager instale la versión más reciente.
6. En Destinos, identifique las instancias en las que desea ejecutar esta operación especificando las etiquetas o seleccione las instancias manualmente.

   > **Note**
   >
   > Si decide seleccionar las instancias manualmente y una de las instancias que desea utilizar no figura en la lista, consulte ¿Dónde están mis instancias? en la Guía del usuario de AWS Systems Manager para obtener sugerencias sobre la solución del problema.

7. En Otros parámetros:
   - (Opcional) En Comentario, escriba la información acerca de este comando.
   - En Tiempo de espera (segundos), especifique el número de segundos que tiene que esperar el sistema antes de indicar que se ha producido un error en la ejecución del comando general.
8. (Opcional) En Control de velocidad:

- En Concurrencia, especifique un número o un porcentaje de las instancias en las que desea ejecutar el comando al mismo tiempo.

  > **Note**
  >
  > Si selecciona destinos mediante la elección de etiquetas Amazon EC2 y no está seguro de cuántas instancias utilizan las etiquetas seleccionadas, limite el número de instancias que puede ejecutar el documento al mismo tiempo. Para ello, especifique un porcentaje.

- En Umbral de errores, especifique cuándo desea parar la ejecución del comando en las demás instancias después de que haya fallado en un número o un porcentaje de las instancias. Por ejemplo, si especifica tres errores, Systems Manager dejará de enviar el comando cuando se reciba el cuarto error. Las instancias que estén procesando el comando todavía pueden enviar errores.

9. (Opcional) En la sección Opciones de salida, si desea guardar la salida del comando en un archivo, seleccione Escribir la salida del comando en un bucket de S3. Especifique el bucket y los nombres de prefijo (carpeta) (opcionales).

   > **Note**
   >
   > Los permisos de S3 que conceden la capacidad de escribir datos en un bucket de S3 son los del perfil de instancia asignado a la instancia, no los del usuario que lleva a cabo esta tarea. Para obtener más información, consulte Crear un perfil de instancias de IAM para Systems Manager en la Guía del usuario de AWS Systems Manager.

10. (Opcional) Especifique las opciones de Notificaciones SNS.

    Para obtener información acerca de la configuración de las notificaciones de Amazon SNS para Run Command, consulte Configuración de las notificaciones de Amazon SNS para AWS Systems Manager.

11. Elija Ejecutar.

AWS CLI

Siga el procedimiento que se indica a continuación para descargar e instalar el paquete de `AwsVssComponents` en sus instancias con Run Command desde la AWS CLI. El paquete

instala dos componentes: un solicitante de VSS y un proveedor de VSS. El sistema copia estos componentes en un directorio de la instancia y, a continuación, registra la DLL del proveedor como proveedor de VSS.

Para instalar el paquete de VSS mediante la AWS CLI

- Ejecute el siguiente comando para descargar e instalar los componentes VSS requeridos para Systems Manager.

```
aws ssm send-command \
  --document-name "AWS-ConfigureAWSPackage" \
  --instance-ids "i-01234567890abcdef" \
  --parameters '{"action":["Install"],"name":["AwsVssComponents"]}'
```

PowerShell

Siga el procedimiento que se indica a continuación para descargar e instalar el paquete de `AwsVssComponents` en sus instancias con Run Command desde las herramientas para Windows PowerShell. El paquete instala dos componentes: un solicitante de VSS y un proveedor de VSS. El sistema copia estos componentes en un directorio de la instancia y, a continuación, registra la DLL del proveedor como proveedor de VSS.

Para instalar el paquete de VSS con AWS Tools for Windows PowerShell

- Ejecute el siguiente comando para descargar e instalar los componentes VSS requeridos para Systems Manager.

```
Send-SSMCommand -DocumentName AWS-ConfigureAWSPackage -InstanceId
 "i-01234567890abcdef" -Parameter
 @{'action'='Install';'name'='AwsVssComponents'}
```

Verificación de la firma en los componentes de VSS de AWS

Utilice el siguiente procedimiento para verificar la firma en el paquete `AwsVssComponents`.

1. Conéctese a la instancia de Windows. Para obtener más información, consulte Conexión con la instancia de Windows de.
2. Vaya a C:\Program Files\Amazon\AwsVssComponents.

3. Abra el menú contextual de `ec2-vss-agent.exe` (con el botón derecho del ratón) y, a continuación, elija Propiedades.
4. Vaya a la pestaña Firmas digitales y compruebe que el nombre del firmante sea Amazon Web Services Inc.
5. Siga los pasos anteriores para verificar la firma en `Ec2VssInstaller` y `Ec2VssProvider.dll`.

Actualización de los componentes de VSS en sus instancias en función de una programación

Le recomendamos que mantenga siempre actualizados los componentes de VSS con la versión más reciente recomendada. Existen varias formas diferentes de actualizar componentes cuando se inicia una nueva versión del paquete `AwsVssComponents`.

Métodos de actualización

- Puede repetir los pasos descritos en Instalación manual de los componentes de VSS en una instancia cuando se publique una nueva versión de los componentes de VSS de AWS.
- Puede configurar una asociación de Systems Manager State Manager para descargar e instalar automáticamente componentes nuevos o actualizados de VSS cuando el paquete `AwsVssComponents` esté disponible.
- Puede instalar o actualizar automáticamente el paquete `AwsVssComponents` siempre que cree instantáneas coherentes con las aplicaciones, cuando utilice Systems Manager para ejecutar el documento `AWSEC2-VssInstallAndSnapshot`.

> **Note**
>
> Se recomienda utilizar Systems Manager para ejecutar el documento de comandos `AWSEC2-VssInstallAndSnapshot`, que instala o actualiza automáticamente el paquete `AwsVssComponents` antes de crear las instantáneas coherentes con las aplicaciones. Para obtener más información, consulte Ejecute el documento de comandos AWSEC2-VssInstallAndSnapshot (recomendado).

Para crear una asociación de Systems Manager State Manager, siga los pasos del entorno que prefiera.

Console

Para crear una asociación de State Manager mediante la consola

1. Abra la consola de AWS Systems Manager en https://console.aws.amazon.com/systems-manager/.
2. En el panel de navegación, elija Administrador de estados.

   O bien, si primero se abre la página de inicio de Systems Manager, abra el panel de navegación y, a continuación, seleccione State Manager.
3. Elija Crear asociación.
4. En el campo Nombre, ingrese un nombre descriptivo.
5. En la lista Documento, elija AWS-ConfigureAWSPackage.
6. En la sección Parámetros, elija Instalar en la lista Acción.
7. En Tipo de instalación, elija Desinstalar y volver a instalar.
8. En el campo Nombre, escriba `AwsVssComponents`. Puede mantener los campos Versión y Argumentos adicionales vacíos.
9. En la sección Destinos, elija una opción.

   > **Note**
   >
   > Si elige dirigirse a las instancias mediante etiquetas y especifica etiquetas que se mapean a instancias de Linux, la asociación se realiza correctamente en la instancia de Windows, pero no en las instancias de Linux. El estado general de la asociación muestra Failed.
10. En la sección Especificar programa, elija una opción.
11. En la sección Opciones avanzadas, en Gravedad de conformidad, elija un nivel de gravedad para la asociación. Para obtener más información, consulte Acerca de la conformidad de las asociaciones de State Manager. En Calendarios de cambios, seleccione un calendario de cambios preconfigurado. Para obtener más información, consulte Calendario de cambios AWS Systems Manager.
12. En Control de velocidad, haga lo siguiente:

    - En Simultaneidad, especifique un número o un porcentaje de los nodos administrados en los que desea ejecutar el comando al mismo tiempo.

- En Umbral de errores, especifique cuándo desea parar la ejecución del comando en los demás nodos administrados después de que haya fallado en un número o un porcentaje de los nodos.

13. (Opcional) En Opciones de salida, para guardar la salida del comando en un archivo, seleccione Permitir la escritura de salida en S3. Ingrese los nombres del bucket y del prefijo (carpeta) en los cuadros.
14. Elija Crear asociación y, a continuación, Cerrar. El sistema intenta crear la asociación en las instancias y aplicar inmediatamente el estado.

> **Note**
>
> Si las instancias de EC2 de Windows Server tienen el estado Error, asegúrese de que SSM Agent se está ejecutando en la instancia y que esta se ha configurado como un rol de AWS Identity and Access Management (IAM) para Systems Manager. Para obtener más información, consulte Configuración de AWS Systems Manager.

AWS CLI

Puede ejecutar el comando de la AWS CLI create-association para actualizar un paquete del Distribuidor de forma programada sin desconectar la aplicación asociada. Solo se reemplazan los archivos nuevos o actualizados del paquete.

Para crear una asociación de State Manager mediante la AWS CLI

1. Si aún no lo ha hecho, instale y configure AWS CLI. Para obtener más información, consulte Instalar o actualizar la última versión de la AWS CLI.
2. Ejecute el siguiente comando para crear una asociación. El valor de `--name`, el nombre del documento, es siempre `AWS-ConfigureAWSPackage`. El comando siguiente utiliza la clave `InstanceIds` para especificar las instancias de destino.

```
aws ssm create-association \
 --name "AWS-ConfigureAWSPackage" \
 --parameters '{"action":["Install"],"installationType":["Uninstall and
 reinstall"],"name":["AwsVssComponents"]}' \
 --targets [{\"Key\":\"InstanceIds\",\"Values\":[\"i-01234567890abcdef\",
\"i-000011112222abcde\"]}]
```

Para obtener más información acerca de otras opciones que puede utilizar con el comando `create-association`, consulte create-association en la sección sobre AWS Systems Manager de la referencia de comandos de la AWS CLI.

Creación de instantáneas de EBS compatibles con VSS

En esta sección se incluyen los pasos para crear instantáneas de EBS compatibles con VSS.

Puede crear instantáneas de EBS compatibles con VSS de los volúmenes de EBS asociados a sus instancias de EC2. Antes de intentar crear una instantánea compatible con VSS, asegúrese de que se cumplen los Requisitos previos.

Temas

- Cree instantáneas de VSS con los documentos de comandos de AWS Systems Manager
- Creación de instantáneas de VSS mediante AWS Backup
- Creación de instantáneas de VSS con Amazon Data Lifecycle Manager

Cree instantáneas de VSS con los documentos de comandos de AWS Systems Manager

Puede usar los documentos de comandos de AWS Systems Manager para crear instantáneas compatibles con VSS. En el siguiente contenido, se presentan los documentos de comandos disponibles y los parámetros de tiempo de ejecución que usan los documentos para crear las instantáneas.

Antes de usar cualquiera de los documentos de comandos de Systems Manager, asegúrese de cumplir con todos los Requisitos previos.

Temas

- Parámetros de los documentos para instantáneas de VSS de Systems Manager
- Ejecute los documentos de comandos para instantáneas de VSS de Systems Manager

Parámetros de los documentos para instantáneas de VSS de Systems Manager

Todos los documentos de Systems Manager que crean instantáneas de VSS usan los siguientes parámetros, excepto cuando se indica lo contrario:

ExcludeBootVolume (cadena, opcional)

Esta configuración excluye volúmenes de arranque del proceso de copia de seguridad si crea instantáneas. Para excluir los volúmenes de arranque de las instantáneas, configure ExcludeBootVolume en `True` y CreateAmi en `False`.

Si crea una AMI para la copia de seguridad, este parámetro se debe establecer en `False`. El valor predeterminado para este parámetro es `False`.

NoWriters (cadena, opcional)

Para excluir los escritores de VSS de la aplicación del proceso de instantáneas, establezca este parámetro en `True`. Excluir los escritores de VSS de la aplicación puede ayudar a resolver los conflictos con los componentes de copia de seguridad de VSS de terceros. El valor predeterminado para este parámetro es `False`.

CopyOnly (cadena, opcional)

Si utiliza la copia de seguridad nativa de SQL Server además de VSS de AWS, llevar a cabo una copia de seguridad de solo copia impide que VSS de AWS interrumpa la cadena de copia de seguridad diferencial nativa. Para realizar una operación de copia de seguridad de solo copia, establezca este parámetro en `True`.

El valor predeterminado de este parámetro es `False`, lo que hace que VSS de AWS realice una operación de copia de seguridad completa.

CreateAmi (cadena, opcional)

Para crear una imagen de máquina de Amazon (AMI) habilitada para VSS para hacer una copia de seguridad de la instancia, establezca este parámetro en `True`. El valor predeterminado de este parámetro es `False`, que en su lugar hace una copia de seguridad de la instancia con una instantánea de EBS.

Para obtener más información sobre la creación de una AMI a partir de una instancia, consulte Creación de una AMI basada en Amazon EBS.

AmiName (cadena, opcional)

Si el estado de CreateAmi es `True`, especifique el nombre de la AMI creada por la copia de seguridad.

description (cadena, opcional)

Especifique una descripción para las instantáneas o la imagen que crea este proceso.

tags (cadena, opcional)

Recomendamos etiquetar las instantáneas e imágenes para localizar y administrar los recursos, por ejemplo, para restaurar los volúmenes a partir de una lista de instantáneas. El sistema agrega la clave `Name`, con un valor en blanco, donde puede indicar el nombre que quiere aplicar a las instantáneas o imágenes de salida.

Si quiere especificar otras etiquetas, separe las etiquetas mediante un punto y coma. Por ejemplo, `Key=Environment,Value=Test;Key=User,Value=TestUser1`.

De manera predeterminada, el sistema agrega las siguientes etiquetas reservadas para las instantáneas e imágenes compatibles con VSS.

- Device: en el caso de las instantáneas compatibles con VSS, este es el nombre de dispositivo del volumen de EBS que captura la instantánea.
- AppConsistent: esta etiqueta indica la creación correcta de una instantánea o AMI compatible con VSS.
- AWSVSSConfig: identifica las instantáneas y las AMI que se crean con compatibilidad con VSS. La etiqueta incluye metadatos, como la versión de `AwsVssComponents`.

> **Warning**
>
> Si se especifica alguna de estas etiquetas reservadas en la lista de parámetros, se producirá un error.

executionTimeout (cadena, opcional)

Especifique el tiempo máximo en segundos para ejecutar el proceso de creación de instantáneas en la instancia o para crear una AMI a partir de la instancia. Al aumentar este tiempo de espera, el comando puede esperar más tiempo hasta que VSS inicie la congelación y complete el etiquetado de los recursos que crea. Este tiempo de espera solo se aplica a los pasos de creación de la instantánea o de la AMI. El paso inicial para instalar o actualizar el paquete `AwsVssComponents` no está incluido en el tiempo de espera.

CollectDiagnosticLogs (cadena, opcional)

Para recopilar más información durante los pasos de creación de la instantánea y la AMI, establezca este parámetro en “`True`”. El valor predeterminado para este parámetro es “`False`”. Los registros de diagnóstico consolidados se guardan como un archivo en formato `.zip` en la siguiente ubicación de la instancia:

`C:\ProgramData\Amazon\AwsVss\Logs\timestamp.zip`

VssVersion (cadena, opcional)

Solo para el documento `AWSEC2-VssInstallAndSnapshot`, puede especificar el parámetro `VssVersion` para instalar una versión específica del paquete `AwsVssComponents` en la instancia. Deje en blanco este parámetro para instalar la versión predeterminada recomendada.

Si la versión especificada del paquete `AwsVssComponents` ya está instalada, el script omite el paso de instalación y procede a realizar el paso de copia de seguridad. Para obtener una lista de las versiones del paquete `AwsVssComponents` y la compatibilidad operativa, consulte Historial de versiones de la solución AWS VSS.

Ejecute los documentos de comandos para instantáneas de VSS de Systems Manager

Puede crear instantáneas de EBS compatibles con VSS con los documentos de comandos de AWS Systems Manager de la siguiente forma.

Ejecute el documento de comandos AWSEC2-VssInstallAndSnapshot (recomendado)

Cuando usa AWS Systems Manager para ejecutar el documento `AWSEC2-VssInstallAndSnapshot`, el script ejecuta los siguientes pasos.

1. El script primero instala o actualiza el paquete `AwsVssComponents` en la instancia, en función de si ya está instalado o no.
2. El script crea las instantáneas coherentes con las aplicaciones una vez finalizado el primer paso.

Para ejecutar el documento `AWSEC2-VssInstallAndSnapshot`, siga los pasos de su entorno de preferencia.

Console

Creación de instantáneas de EBS compatibles con VSS desde la consola

1. Abra la consola de AWS Systems Manager en https://console.aws.amazon.com/systems-manager/.
2. En el panel de navegación, seleccione Ejecutar comando. Se muestra una lista de los comandos que se están ejecutando actualmente en su cuenta, si corresponde.
3. Elija Run command (Ejecutar comando). Se abre una lista de documentos de comandos a los que tiene acceso.

4. Seleccione `AWSEC2-VssInstallAndSnapshot` de la lista de documentos de comandos. Para agilizar los resultados, puede ingresar todo el nombre del documento o una parte. También puede filtrar por propietario, por tipo de plataforma o por etiquetas.

   Al seleccionar un documento de comandos, los detalles aparecen debajo de la lista.

5. Seleccione `Default version at runtime` de la lista Versión del documento.
6. Configure Parámetros de comando para definir cómo `AWSEC2-VssInstallAndSnapshot` instalará el paquete `AwsVssComponents` y realizará la copia de seguridad con una AMI o instantáneas de VSS. Para obtener detalles sobre los parámetros, consulte Parámetros de los documentos para instantáneas de VSS de Systems Manager.
7. En Selección de destino, especifique las etiquetas o seleccione manualmente las instancias para identificar las instancias en las que ejecutar esta operación.

   > **Note**
   >
   > Si selecciona las instancias manualmente y una de las instancias que desea utilizar no figura en la lista, consulte ¿Dónde están mis instancias? para ver cómo resolver el problema.

8. Para obtener parámetros adicionales que definan el comportamiento de Systems Manager Run Command, como Control de velocidad, ingrese los valores descritos en Ejecución de comandos desde la consola.
9. Elija Run (Ejecutar).

   Si todo sale bien, el comando rellena la lista de instantáneas de EBS con las nuevas instantáneas. Puede encontrar estas instantáneas en la lista de instantáneas de EBS buscando las etiquetas que especificó o `AppConsistent`. Si se ha producido un error en la ejecución de comandos, consulte la información de salida del comando de Systems Manager para obtener detalles acerca de por qué se ha producido un error en la ejecución. Si el comando se ha completado correctamente, pero se ha producido un error en un backup de volumen específico, puede solucionar el error en la lista de volúmenes de EBS.

AWS CLI

Puede ejecutar los siguientes comandos en la AWS CLI para crear instantáneas de EBS compatibles con VSS y obtener el estado de la creación de la instantánea.

Creación de instantáneas de EBS compatibles con VSS

Para crear instantáneas de EBS compatibles con VSS, ejecute el siguiente comando. Para crear las instantáneas, debe identificar las instancias con el parámetro `--instance-ids`. Para obtener más información acerca de otros parámetros que puede usar, consulte Parámetros de los documentos para instantáneas de VSS de Systems Manager.

```
aws ssm send-command \
 --document-name "AWSEC2-VssInstallAndSnapshot" \
 --instance-ids "i-01234567890abcdef" \
 --parameters '{"ExcludeBootVolume":["False"],"description":["Description"],"tags":
["Key=key_name,Value=tag_value"],"VssVersion":[""]}'
```

Si todo sale bien, el documento de comando rellena la lista de instantáneas de EBS con las nuevas instantáneas. Puede encontrar estas instantáneas en la lista de instantáneas de EBS buscando las etiquetas que especificó o `AppConsistent`. Si se ha producido un error en la ejecución de comandos, consulte la información de salida del comando de para obtener detalles acerca de por qué se ha producido un error en la ejecución.

Obtener el estado del comando

Para obtener el estado actual de las instantáneas, ejecute el siguiente comando con el ID de comando devuelto de send-command.

```
aws ssm get-command-invocation
 --instance-ids "i-01234567890abcdef" \
 --command-id "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
 --plugin-name "CreateVssSnapshot"
```

PowerShell

Ejecute los siguientes comandos con AWS Tools for Windows PowerShell para crear instantáneas de EBS compatibles con VSS y obtener el estado de tiempo de ejecución actual de la creación de la salida. Especifique los parámetros descritos en la lista anterior para modificar el comportamiento del procesamiento de instantáneas.

Creación de instantáneas de EBS compatibles con VSS mediante Herramientas para Windows PowerShell

Ejecute el siguiente comando para crear AMI o instantáneas de EBS compatibles con VSS.

```
Send-SSMCommand -DocumentName "AWSEC2-VssInstallAndSnapshot" -InstanceId
 "i-01234567890abcdef" -Parameter
 @{'ExcludeBootVolume'='False';'description'='a_description'
 ;'tags'='Key=key_name,Value=tag_value';'VssVersion'=''}
```

Obtener el estado del comando

Para obtener el estado actual de las instantáneas, ejecute el siguiente comando con el ID de comando devuelto de Send-SSMCommand.

```
Get-SSMCommandInvocationDetail -InstanceId "i-01234567890abcdef" -CommandId
 "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" -PluginName "CreateVssSnapshot"
```

Si todo sale bien, el comando rellena la lista de instantáneas de EBS con las nuevas instantáneas. Puede encontrar estas instantáneas en la lista de instantáneas de EBS buscando las etiquetas que especificó o `AppConsistent`. Si se ha producido un error en la ejecución de comandos, consulte la información de salida del comando de para obtener detalles acerca de por qué se ha producido un error en la ejecución.

Ejecute el documento de comandos AWSEC2-CreateVssSnapshot

Para ejecutar el documento `AWSEC2-CreateVssSnapshot`, siga los pasos de su entorno de preferencia.

Console

Creación de instantáneas de EBS compatibles con VSS desde la consola

1. Abra la consola de AWS Systems Manager en https://console.aws.amazon.com/systems-manager/.
2. En el panel de navegación, seleccione Ejecutar comando. Se muestra una lista de los comandos que se están ejecutando actualmente en su cuenta, si corresponde.
3. Elija Run command (Ejecutar comando). Se abre una lista de documentos de comandos a los que tiene acceso.
4. Seleccione `AWSEC2-CreateVssSnapshot` de la lista de documentos de comandos. Para agilizar los resultados, puede ingresar todo el nombre del documento o una parte. También puede filtrar por propietario, por tipo de plataforma o por etiquetas.

Al seleccionar un documento de comandos, los detalles aparecen debajo de la lista.

5. Seleccione `Default version at runtime` de la lista Versión del documento.
6. Configure los Parámetros de comando para definir cómo `AWSEC2-CreateVssSnapshot` realizará la copia de seguridad con instantáneas de VSS o con una AMI. Para obtener detalles sobre los parámetros, consulte Parámetros de los documentos para instantáneas de VSS de Systems Manager.
7. En Selección de destino, especifique las etiquetas o seleccione manualmente las instancias para identificar las instancias en las que ejecutar esta operación.

   > **Note**
   >
   > Si selecciona las instancias manualmente y una de las instancias que desea utilizar no figura en la lista, consulte ¿Dónde están mis instancias? para ver cómo resolver el problema.

8. Para obtener parámetros adicionales que definan el comportamiento de Systems Manager Run Command, como Control de velocidad, ingrese los valores descritos en Ejecución de comandos desde la consola.
9. Elija Run (Ejecutar).

   Si todo sale bien, el comando rellena la lista de instantáneas de EBS con las nuevas instantáneas. Puede encontrar estas instantáneas en la lista de instantáneas de EBS buscando las etiquetas que especificó o `AppConsistent`. Si se ha producido un error en la ejecución de comandos, consulte la información de salida del comando de Systems Manager para obtener detalles acerca de por qué se ha producido un error en la ejecución. Si el comando se ha completado correctamente, pero se ha producido un error en un backup de volumen específico, puede solucionar el error en la lista de volúmenes de EBS.

AWS CLI

Puede ejecutar el siguiente comando en la AWS CLI para crear instantáneas de EBS compatibles con VSS.

Creación de instantáneas de EBS compatibles con VSS

Para crear instantáneas de EBS compatibles con VSS, ejecute el siguiente comando. Para crear las instantáneas, debe identificar las instancias con el parámetro `--instance-ids`. Para

obtener más información acerca de otros parámetros que puede usar, consulte Parámetros de los documentos para instantáneas de VSS de Systems Manager.

```
aws ssm send-command \
 --document-name "AWSEC2-CreateVssSnapshot" \
 --instance-ids "i-01234567890abcdef" \
 --parameters '{"ExcludeBootVolume":["False"],"description":["Description"],"tags":
["Key=key_name,Value=tag_value"]}'
```

Si todo sale bien, el documento de comando rellena la lista de instantáneas de EBS con las nuevas instantáneas. Puede encontrar estas instantáneas en la lista de instantáneas de EBS buscando las etiquetas que especificó o `AppConsistent`. Si se ha producido un error en la ejecución de comandos, consulte la información de salida del comando de para obtener detalles acerca de por qué se ha producido un error en la ejecución.

PowerShell

Para crear instantáneas de EBS compatibles con VSS, ejecute el siguiente comando con AWS Tools for Windows PowerShell.

Creación de instantáneas de EBS compatibles con VSS mediante Herramientas para Windows PowerShell

Para crear instantáneas de EBS compatibles con VSS, ejecute el siguiente comando. Para crear las instantáneas, debe identificar las instancias con el parámetro `InstanceId`. Puede especificar más de una instancia para crear instantáneas. Para obtener más información acerca de otros parámetros que puede usar, consulte Parámetros de los documentos para instantáneas de VSS de Systems Manager.

```
Send-SSMCommand -DocumentName AWSEC2-CreateVssSnapshot -InstanceId
 "i-01234567890abcdef" -Parameter
 @{'ExcludeBootVolume'='False';'description'='a_description'
 ;'tags'='Key=key_name,Value=tag_value'}
```

Si todo sale bien, el comando rellena la lista de instantáneas de EBS con las nuevas instantáneas. Puede encontrar estas instantáneas en la lista de instantáneas de EBS buscando las etiquetas que especificó o `AppConsistent`. Si se ha producido un error en la ejecución de comandos, consulte la información de salida del comando de para obtener detalles acerca de por qué se ha producido un error en la ejecución. Si el comando se ha completado correctamente,

pero se ha producido un error en una copia de seguridad de volumen específico, puede solucionar el error en la lista de instantáneas de EBS.

Ejecución de los documentos de comandos en un clúster de conmutación por error de Windows con almacenamiento EBS compartido

Puede usar cualquiera de los procedimientos de línea de comandos descritos en la sección anterior para crear una instantánea compatible con VSS. El documento de comandos (`AWSEC2-VssInstallAndSnapshot` o `AWSEC2-CreateVssSnapshot`) debe ejecutarse en el nodo principal del clúster. El documento fallará en los nodos secundarios, ya que no tienen acceso a los discos compartidos. Si el comando principal y el secundario cambian de forma dinámica, puede ejecutar el documento Ejecutar comandos de AWS Systems Manager en varios nodos con la expectativa de que el comando se ejecute correctamente en el nodo principal y falle en los nodos secundarios.

Ejecute el documento de comandos AWSEC2-ManageVssIO de SSM

Puede utilizar el siguiente script y el documento predefinido de SSM `AWSEC2-ManageVssIO` para detener de forma temporal las E/S, crear instantáneas de EBS compatibles con VSS y reiniciar las E/S. Este proceso se ejecuta en el contexto del usuario que ejecuta el comando. Si el usuario tiene permisos suficientes para crear y etiquetar instantáneas, AWS Systems Manager puede crear y etiquetar instantáneas de EBS compatibles con VSS sin la necesidad de contar con el rol adicional de la instantánea de IAM en la instancia.

Por el contrario, el documento de comandos (`AWSEC2-VssInstallAndSnapshot` o `AWSEC2-CreateVssSnapshot`) requiere que asigne el rol de la instantánea de IAM a cada instancia para la que quiera crear instantáneas de EBS. Si no desea proporcionar permisos de IAM adicionales a las instancias por motivos de política o conformidad, puede usar el siguiente script.

Antes de empezar

Tenga en cuenta los siguientes detalles importantes acerca de este proceso:

- Este proceso usa un script de PowerShell (`CreateVssSnapshotAdvancedScript.ps1`) para tomar instantáneas de todos los volúmenes en las instancias que especifique, salvo volúmenes raíz. Si necesita tomar instantáneas de volúmenes raíz, debe usar el documento de SSM `AWSEC2-CreateVssSnapshot`.
- El script llama al documento `AWSEC2-ManageVssIO` dos veces. La primera vez con el parámetro `Action` establecido en `Freeze`, que detiene toda la E/S en las instancias. La segunda vez, el parámetro `Action` se establece en `Thaw`, que fuerza la reanudación de la E/S.

- No intente usar el documento `AWSEC2-ManageVssIO` sin utilizar el script CreateVssSnapshotAdvancedScript.ps1. El marco de VSS de Microsoft requiere que no se llame a las acciones `Freeze` y `Thaw` con más de diez segundos de diferencia, mientras que llamar manualmente a estas acciones sin el script podría dar lugar a errores.

Para crear instantáneas de EBS compatibles con VSS mediante el documento de SSM **`AWSEC2-ManageVssIO`**

1. Descargue el archivo CreateVssSnapshotAdvancedScript.zip y extraiga su contenido.
2. Abra `CreateVssSnapshotAdvancedScript.ps1` en un editor de texto, edite el ejemplo de llamada al final del script con un ID de instancia de EC2 válido, la descripción de la instantánea y los valores de etiquetas deseados, y luego ejecute el script desde PowerShell.

Si todo sale bien, el comando rellena la lista de instantáneas de EBS con las nuevas instantáneas. Puede encontrar estas instantáneas en la lista de instantáneas de EBS buscando las etiquetas que especificó o `AppConsistent`. Si se ha producido un error en la ejecución de comandos, consulte la información de salida del comando de para obtener detalles acerca de por qué se ha producido un error en la ejecución. Si el comando se ha completado correctamente, pero se ha producido un error en una copia de seguridad de volumen específico, puede solucionar el error en la lista de volúmenes de EBS.

> **Note**
>
> Para automatizar las copias de seguridad, puede crear una tarea de periodo de mantenimiento de AWS Systems Manager que use el documento `AWSEC2-VssInstallAndSnapshot`. Para obtener más información, consulte Trabajo con periodos de mantenimiento (Consola) en la Guía del usuario de AWS Systems Manager.

Creación de instantáneas de VSS mediante AWS Backup

Puede crear una copia de seguridad de VSS cuando utilice AWS Backup si habilita VSS en la consola o en la CLI. Asegúrese de cumplir con los requisitos previos antes de crear el plan de copia de seguridad compatible con VSS. Para obtener más información, consulte Creación de copias de seguridad de Windows VSS en la Guía para desarrolladores de AWS Backup.

> **Note**
>
> AWS Backup no instala automáticamente el paquete `AwsVssComponents` en la instancia. Debe realizar una instalación manual en la instancia. Para obtener más información, consulte Instalación manual de los componentes de VSS en una instancia.

Creación de instantáneas de VSS con Amazon Data Lifecycle Manager

Para crear instantáneas de VSS con Amazon Data Lifecycle Manager, puede habilitar scripts previos y posteriores en sus políticas de ciclo de vida de instantáneas. Para obtener más información, consulte https://docs.aws.amazon.com/ebs/latest/userguide/automate-app-consistent-backups.html.

> **Note**
>
> Amazon Data Lifecycle Manager no instala automáticamente el paquete `AwsVssComponents` en la instancia. Debe realizar una instalación manual en la instancia. Para obtener más información, consulte Instalación manual de los componentes de VSS en una instancia.

Solucione problemas con las instantáneas de EBS basadas en VSS de Windows

Antes de intentar cualquier otro paso de solución de problemas, le recomendamos que compruebe los siguientes detalles.

- Asegúrese de cumplir con todos Requisitos previos.
- Compruebe que esté usando el Compatibilidad de versiones del sistema operativo Windows más reciente del paquete `AwsVssComponents` para su sistema operativo. Es posible que el problema que ha observado se haya solucionado en versiones más recientes.

Temas

- Controlar los archivos de registro
- Recopilar registros de diagnóstico adicionales
- Utilización de VSS en instancias con proxy configurado

- Error: tiempo de espera de conexión de canalización de descongelación, error al descongelar, tiempo de espera de congelación de VSS u otros errores de tiempo de espera.
- Error: no se puede invocar el método. La invocación de métodos solo se admite en tipos principales en este modo de lenguaje

Controlar los archivos de registro

Si tiene problemas o recibe mensajes de error al crear instantáneas de EBS compatibles con VSS, puede ver la salida de los comandos en la consola de Systems Manager.

Para los documentos de Systems Manager que crean instantáneas de VSS, puede establecer el parámetro `CollectDiagnosticLogs` en "`True`" en el tiempo de ejecución. Cuando el parámetro `CollectDiagnosticLogs` se establece en "`True`", VSS recopila registros adicionales para facilitar la depuración. Para obtener más información, consulte Recopilar registros de diagnóstico adicionales.

Si recopila registros de diagnóstico, el documento Systems Manager los almacena en la instancia en la siguiente ubicación: `C:\ProgramData\Amazon\AwsVss\Logs\`*`timestamp`*`.zip`. El valor predeterminado para el parámetro `CollectDiagnosticLogs` es "`False`".

> **Note**
>
> Para obtener ayuda adicional con la depuración, puede enviar el archivo `.zip` al AWS Support.

Los siguientes registros adicionales están disponibles, ya sea si recopila registros de diagnóstico o no:

- `%ProgramData%\Amazon\SSM\InstanceData\`*`InstanceID`*`\document\orchestration\`*`SSMCommandID`*`\awsrunPowerShellScript\runPowerShellScript\stdout`
- `%ProgramData%\Amazon\SSM\InstanceData\`*`InstanceID`*`\document\orchestration\`*`SSMCommandID`*`\awsrunPowerShellScript\runPowerShellScript\stderr`

También puede abrir la aplicación del visor de eventos de Windows y seleccionar la aplicación de Registros de Windows para ver registros adicionales. Para ver eventos específicos del proveedor

de VSS de EC2 para Windows y el servicio Volume Shadow Copy Service, filtre por Origen en los términos **`Ec2VssSoftwareProvider`** y **`VSS`**.

Si utiliza Systems Manager con puntos de conexión de VPC y la acción de API SendCommand de Systems Manager (o Ejecutar comando en la consola) falló, verifique que haya configurado de manera correcta el siguiente punto de conexión: com.amazonaws.***`region`***.ec2.

Si el punto de conexión de Amazon EC2 no está definido, se produce un error en la llamada para enumerar los volúmenes de EBS asociados, lo que hace que el comando de Systems Manager no se ejecute correctamente. Para obtener más información acerca de la configuración de los puntos de conexión de VPC con Systems Manager, consulte Crear un punto de conexión de la nube virtual privada en la Guía del usuario de AWS Systems Manager.

Recopilar registros de diagnóstico adicionales

Para recopilar registros de diagnóstico adicionales con el comando de envío de Systems Manager para ejecutar el documento de instantáneas del VSS, defina el parámetro de entrada `CollectDiagnosticLogs` en “`True`” en el tiempo de ejecución. Se recomienda que establezca el parámetro en “`True`” al corregir los errores.

Para ver el ejemplo de línea de comando, seleccione una de las siguientes pestañas.

AWS CLI

El siguiente ejemplo ejecuta el documento de Systems Manager `AWSEC2-CreateVssSnapshot` en AWS CLI:

```
aws ssm send-command \
--document-name "AWSEC2-CreateVssSnapshot" \
--instance-ids "i-1234567890abcdef0" \
--parameters '{"description":["Example - create diagnostic logs at
 runtime."],"tags":["Key=tag_name,Value=tag_value"],"CollectDiagnosticLogs":
["True"]}'
```

PowerShell

El siguiente ejemplo ejecuta el documento de Systems Manager `AWSEC2-CreateVssSnapshot` en PowerShell:

```
Send-SSMCommand -DocumentName AWSEC2-CreateVssSnapshot -InstanceId
 "i-1234567890abcdef0" -Parameter @{'description'='Example - create diagnostic logs
 at runtime.';'tags'='Key=tag_name,Value=tag_value';'CollectDiagnosticLogs'='True'}
```

Utilización de VSS en instancias con proxy configurado

Si tiene problemas al crear instantáneas de EBS compatibles con VSS en instancias que utilizan un proxy para llegar a los puntos de conexión de EC2, asegúrese de lo siguiente:

- El proxy se configura para que se pueda acceder a los puntos de conexión del servicio EC2 de la región y el IMDS de la instancia mediante la ejecución de AWS Tools for Windows PowerShell como SYSTEM.
- Se ha instalado la versión 2.0.1 o posterior de `AwsVssComponents`. A partir de la versión 2.0.1 de `AwsVssComponents`, el proveedor de VSS de EC2 admite el uso del proxy WinHTTP configurado del sistema. Para obtener más información acerca de la configuración del proxy WinHTTP, consulte Netsh Commands for Windows Hypertext Transfer Protocol (WINHTTP) en el sitio web de Microsoft.

Error: tiempo de espera de conexión de canalización de descongelación, error al descongelar, tiempo de espera de congelación de VSS u otros errores de tiempo de espera.

El proveedor de VSS de EC2 para Windows puede agotar el tiempo de espera debido a la actividad o los servicios en la instancia que impiden que las instantáneas habilitadas para VSS se lleven a cabo de manera oportuna. Windows VSS Framework proporciona una ventana de 10 segundos no configurable durante la cual se pausa la comunicación con el sistema de archivos. Durante este tiempo, `AWSEC2-CreateVssSnapshot` crea instantáneas de los volúmenes.

Los siguientes problemas pueden hacer que el proveedor de VSS de EC2 para Windows se ejecute dentro de límites de tiempo durante una instantánea:

- Exceso de E/S a un volumen
- Capacidad de respuesta lenta de la API de EC2 en la instancia
- Volúmenes fragmentados
- Incompatibilidad con algún software antivirus
- Problemas con un escritor de aplicaciones de VSS

- Cuando el registro de módulos está habilitado para un gran número de módulos de PowerShell, esto puede hacer que los scripts de PowerShell se ejecuten lentamente.

La mayoría de los problemas de tiempo de espera que se encuentran al ejecutar el documento de comandos `AWSEC2-CreateVssSnapshot` están relacionados con que la carga de trabajo en la instancia es demasiado alta en el momento de realizar la copia de seguridad. Las siguientes acciones pueden ayudarlo a realizar una instantánea correcta:

- Vuelva a intentar el comando `AWSEC2-CreateVssSnapshot` para ver si el intento de instantánea se realiza correctamente. Si el reintento se realiza correctamente en algunos casos, la reducción de la carga de instancias podría hacer que las instantáneas sean más exitosas.
- Espere un momento a que disminuya la carga de trabajo de la instancia y vuelva a intentar el comando `AWSEC2-CreateVssSnapshot`. Alternativamente, puede intentar hacer instantáneas cuando se sabe que la instancia está con tensión baja.
- Intente hacer instantáneas de VSS cuando el software antivirus del sistema esté apagado. Si esto resuelve el problema, consulte las instrucciones del software antivirus y configúrelo para permitir instantáneas de VSS.
- Si hay un gran volumen de llamadas a la API de Amazon EC2 en su cuenta dentro de la misma región en la que está ejecutando una instantánea, la limitación de la API podría retrasar las operaciones de la instantánea. Para reducir el impacto de las limitaciones, use el paquete `AwsVssComponents` más reciente (versión 2.1.0 o superior, con los requisitos previos). Este paquete usa la acción de la API `CreateSnapshots` de EC2 para reducir el número de acciones mutantes, como la creación de instantáneas por volumen y el etiquetado.
- Si tiene varios scripts de comandos de `AWSEC2-CreateVssSnapshot` ejecutándose al mismo tiempo, puede seguir los siguientes pasos para reducir los problemas de simultaneidad.
  - Considere la posibilidad de programar las instantáneas durante los periodos de menor actividad de la API.
  - Si usa Run Command en la consola de Systems Manager (o SendCommand en la API) para ejecutar el script de comandos, puede usar los controles de velocidad de Systems Manager para reducir la simultaneidad.

    También puede usar los controles de velocidad de Systems Manager para reducir la simultaneidad de servicios como AWS Backup que usan Systems Manager para ejecutar el script de comandos.

- Ejecute el comando `vssadmin list writers` en un shell y vea si informa algún error en el campo Último error para cualquier escritor del sistema. Si algún escritor informa de un error de tiempo de espera, considere reintentar hacer instantáneas cuando la instancia esté con menos carga.
- Cuando usa tipos de instancias más pequeños, como *t2 | t3 | t3a*.nano o *t2 | t3 | t3a*.micro, pueden producirse tiempos de espera debidos a limitaciones de memoria y CPU. Las siguientes acciones pueden ayudar a reducir los problemas de tiempo de espera.
  - Intente cerrar las aplicaciones que consumen mucha memoria o CPU antes de tomar instantáneas.
  - Intente tomar instantáneas durante los periodos de menor actividad de las instancias.

Error: no se puede invocar el método. La invocación de métodos solo se admite en tipos principales en este modo de lenguaje

Encontrará este error cuando el modo de lenguaje de PowerShell no esté configurado en `FullLanguage`. Los documentos de SSM `AWSEC2-CreateVssSnapshot` y `AWSEC2-ManageVssIo` requieren que PowerShell esté configurado en modo `FullLanguage`.

Para verificar el modo de lenguaje, ejecute el siguiente comando en la instancia en una consola de PowerShell:

```
$ExecutionContext.SessionState.LanguageMode
```

Para obtener más información acerca de los modos de lenguaje, consulte About_Language_Modes en la documentación de Microsoft.

Restauración de volúmenes de EBS desde instantáneas de EBS compatibles con VSS

Puede utilizar el script `RestoreVssSnapshotSampleScript.ps1` para restaurar volúmenes en una instancia desde instantáneas de EBS compatibles con VSS. Este script realiza las siguientes tareas:

- Detiene una instancia
- Quita todas las unidades existentes de la instancia (salvo el volumen de arranque, en caso de haberse excluido)
- Crea nuevos volúmenes a partir de las instantáneas

- Asocia los volúmenes a la instancia mediante la etiqueta de ID de dispositivo en la instantánea
- Reinicia la instancia

> **Important**
>
> El siguiente script desvincula todos los volúmenes asociados a una instancia y, a continuación, crea nuevos volúmenes a partir de una instantánea. Asegúrese de que ha realizado correctamente la copia de seguridad de la instancia. Los volúmenes anteriores no se eliminan. Si lo desea, puede editar el script para eliminar los volúmenes anteriores.

Para restaurar volúmenes desde instantáneas de EBS compatibles con VSS

1. Descargue el archivo RestoreVssSnapshotSampleScript.zip y extraiga su contenido.
2. Abra `RestoreVssSnapshotSampleScript.ps1` en un editor de texto, edite el ejemplo de llamada al final del script con un ID de instancia de EC2 y un ID de instantánea de EBS válidos y luego ejecute el script desde PowerShell.

Historial de versiones de la solución AWS VSS

Temas

- Versiones del paquete AwsVssComponents
- Compatibilidad de versiones del sistema operativo Windows

Versiones del paquete AwsVssComponents

En la siguiente tabla se describen las versiones publicadas del paquete de componentes de AWS VSS.

Versión	Detalles	Fecha de la versión
2.3.2	Se corrigió un caso en el que el registro del proveedor de VSS no se eliminaba al desinstalarlo.	9 de mayo de 2024

Versión	Detalles	Fecha de la versión
2.3.1	Se agregó una nueva etiqueta predeterminada `AwsVssConfig` para identificar las instantáneas y las AMI creadas por AWS VSS.	7 de marzo de 2024
2.2.1	• Se ha agregado compatibilidad con el uso de la API `DescribeInstanceAttribute` . • Correcciones de errores y mejoras de fiabilidad. • Compatibilidad obsoleta con Windows Server 2012 y 2012 R2. AWS No se podrá instalar la versión 2.2.1 de los componentes de VSS en Windows Server 2012 y 2012 R2. AWS La versión 2.1.0 de los componentes de VSS es la última versión compatible con Windows Server 2012 y 2012 R2.	18 de enero de 2024
2.1.0	Se ha agregado compatibilidad con el uso de la API `CreateSnapshots` .	6 de noviembre de 2023
2.0.1	Se agregó compatibilidad para usar la configuración del proxy WinHTTP.	26 de octubre de 2023
2.0.0	Se agregó la capacidad del componente de VSS de AWS para crear instantáneas y AMI, lo que permite la compatibilidad con las características de registro de módulos de PowerShell, registro de bloques de scripts y transcripción.	28 de abril de 2023
1.3.2.0	Se ha corregido un caso en que el error de instalación no se notificaba correctamente.	10 de mayo de 2022

Versión	Detalles	Fecha de la versión
1.3.1.0	• Se han corregido las instantáneas que producían un error en los controladores de dominio debido a un error de registro del escritor VSS de NTDS. • Se ha corregido un error del agente de VSS al desinstalar el proveedor de VSS, versión 1.0.	6 de febrero de 2020
1.3.00	• Se ha mejorado el registro reduciendo la información no deseada. • Se han solucionado los problemas de configuración regional durante la instalación. • Se han corregido los códigos devueltos para algunas condiciones de error del registro de proveedores • Se han solucionado varios problemas de instalación.	19 de marzo de 2019
1.2.00	• Se han agregado parámetros de la línea de comandos `-nw` (sin escritores) y `-copy` (solo copia) al agente. • Se han corregido los errores de EventLog causados por llamadas incorrectas de asignación de memoria	15 de noviembre de 2018
1.1	Se corrigió el uso incorrecto de los componentes de VSS de AWS como el proveedor predeterminado de copia de seguridad y restauración de Windows.	12 de diciembre de 2017
1.0	Versión inicial.	20 de noviembre de 2017

Compatibilidad de versiones del sistema operativo Windows

En la tabla siguiente se muestran las versiones de la solución AWS VSS que hay que ejecutar con cada versión de Windows Server en Amazon EC2.

Versión de Windows Server	Versión de AwsVssComponents	Nombre de la versión de AWSEC2-VssInstallAndSnapshot	Nombre de la versión de AWSEC2-CreateVssSnapshot	Nombre de la versión de AWSEC2-ManageVssIO
Windows Server 2022	predeterminada	predeterminada	predeterminada	predeterminada
Windows Server 2019	predeterminada	predeterminada	predeterminada	predeterminada
Windows Server 2016	predeterminada	predeterminada	predeterminada	predeterminada
Windows Server 2012 R2	2.1.0	no admitido	2012R2	2012R2
Windows Server 2012	2.1.0	no admitido	2012R2	2012R2
Windows Server 2008 R2	1.3.1.0	no admitido	2008R2	2008R2

Prevención de errores de escritura para instancias de Linux

> **Note**
>
> La prevención de errores de escritura solo es compatible con las instancias de Linux.

La prevención de errores de escritura es una característica de almacenamiento en bloque diseñada por AWS para mejorar el rendimiento de las cargas de trabajo de bases de datos relacionales de E/S intensivas y reducir la latencia sin afectar negativamente a la resiliencia de datos. Las bases de datos relacionales que utilizan InnoDB o XtraDB como motor de base de datos, como MySQL y MariaDB, se beneficiarán de la prevención de errores de escritura.

Normalmente, las bases de datos relacionales que utilizan páginas más grandes que la atomicidad por cortes de corriente del dispositivo de almacenamiento utilizan mecanismos de registro de datos para protegerse contra errores de escritura. MariaDB y MySQL utilizan un archivo búfer de doble escritura para registrar los datos antes de escribirlos en las tablas de datos. En caso de escrituras incompletas o con errores, como consecuencia de caídas del sistema operativo o pérdidas de corriente durante las transacciones de escritura, la base de datos puede recuperar los datos del búfer de doble escritura. La sobrecarga adicional de E/S asociada a la escritura en el búfer de doble escritura afecta al rendimiento de la base de datos y a la latencia de la aplicación. También reduce el número de transacciones que pueden procesarse por segundo. Para obtener más información sobre el búfer de doble escritura, consulte la documentación de MariaDB y MySQL.

Con la prevención de errores de escritura, los datos se escriben en el almacenamiento en transacciones de escritura de todo o nada, lo que elimina la necesidad de utilizar el búfer de doble escritura. Esto evita que se escriban datos parciales o con errores en el almacenamiento en caso de una caída del sistema operativo o pérdida de energía durante las transacciones de escritura. El número de transacciones procesadas por segundo puede aumentar hasta un 30 % y la latencia de escritura se puede reducir hasta un 50 %, sin comprometer la resistencia de las cargas de trabajo.

Precios

No hay costos adicionales por utilizar la prevención de errores de escritura.

Tamaños de bloque y alineaciones de límites de bloque admitidos

La prevención de errores de escritura admite operaciones de escritura para bloques de datos de 4 KiB, 8 KiB y 16 KiB. La dirección de bloque lógico (LBA) del inicio de bloque de datos debe estar

alineada con el tamaño del límite de bloque respectivo de 4 KiB, 8 KiB o 16 KiB. Por ejemplo, para operaciones de escritura de 16 KiB, la LBA del inicio de bloque de datos debe alinearse con un tamaño del límite de bloque de 16 KiB.

En la tabla siguiente, se muestra la compatibilidad entre tipos de almacenamiento e instancias.

	bloques de 4 KiB	bloques de 8 KiB	bloques de 16 KiB
Volúmenes de almacén de instancias	Todos los volúmenes de almacenes de instancias de NVMe asociados a instancias de la familia I de la generación actual.	instancias I4i, Im4gn e Is4gen compatibles con Nitro SSD de AWS.	
Volúmenes de Amazon EBS	Todos los volúmenes de Amazon EBS asociados a instancias integradas en el AWS Nitro System.		

Para confirmar si la instancia y el volumen admiten la prevención de errores de escritura, haga una consulta para comprobarlo y para conocer otros detalles, como cuáles son los tamaños de bloque y límite admitidos. Para obtener más información, consulte Comprobar la compatibilidad y la configuración de la prevención de errores de escritura.

Requisitos

Para que la prevención de errores de escritura funcione correctamente, una operación de E/S debe cumplir los requisitos de tamaño, alineación y límites, tal y como se especifica en los campos `NTWPU`, `NTWGU` y `NTWBU`. Debe configurar su sistema operativo para garantizar que el subsistema de almacenamiento específico (sistema de archivos, LVM, RAID, etc.) no modifique las propiedades de E/S en la pila de almacenamiento (lo que incluye fusiones de bloques, divisiones o reubicación de direcciones de bloques) antes de que se envíen al dispositivo.

La prevención de errores de escritura se probó con la configuración siguiente:

- Un tipo de instancia y un tipo de almacenamiento que admiten el tamaño de bloque necesario.
- Amazon Linux 2 con la versión del kernel 5.10 o posterior.
- ext4 con `bigalloc` habilitado y un tamaño de clúster de 16 KiB, y las utilidades de ext4 más recientes (e2fsprogs 1.46.5 o posterior).

- Modo de acceso a archivos `O_DIRECT` para eludir la caché de búfer del kernel de Linux.

> **Note**
>
> No es necesario desactivar la fusión de E/S para cargas de trabajo de MySQL y MariaDB.

Comprobar la compatibilidad y la configuración de la prevención de errores de escritura

Para confirmar si su instancia y volumen admiten la prevención de errores de escritura y para ver los datos específicos del proveedor del espacio de nombres de NVMe que contienen información sobre la prevención de errores de escritura, utilice el siguiente comando.

```
$ sudo nvme id-ns -v device_name
```

> **Note**
>
> El comando devuelve la información específica del proveedor en hexadecimal con interpretación ASCII. Es posible que tenga que crear una herramienta, similar a `ebsnvme-id`, en las aplicaciones que pueda leer y analizar la salida.

Por ejemplo, el siguiente comando devuelve los datos específicos del proveedor del espacio de nombres de NVMe que contienen información de prevención de errores de escritura para `/dev/nvme1n1`.

```
$ sudo nvme id-ns -v /dev/nvme1n1
```

Si su instancia y volumen admiten la prevención de errores de escritura, devuelve la siguiente información de prevención de errores de escritura de AWS en los datos específicos del proveedor del espacio de nombres de NVMe.

> **Note**
>
> Los bytes de la siguiente tabla representan el desplazamiento en bytes desde el principio de los datos específicos del proveedor del espacio de nombres de NVMe.

Bytes	Descripción
0:31	El nombre del punto de montaje del adjunto del dispositivo, como, por ejemplo, /dev/xvda . Se proporciona durante la solicitud de adjunto de volumen y lo puede utilizar la instancia de Amazon EC2 para crear un enlace simbólico al dispositivo de bloques NVMe (nvmeXn1).
32:63	El ID del volumen. Por ejemplo, vol01234567890abcdef . Este campo se puede utilizar para asignar el dispositivo NVMe al volumen adjunto.
64:255	Reservado para uso futuro.
256:257	Tamaño de la unidad de prevención de errores de escritura en el espacio de nombres (NTWPU). Este campo indica el tamaño específico del espacio de nombres de la operación de escritura garantizada que se escribirá atómicamente en NVM durante un corte de corriente o una condición de error. Este campo se especifica en bloques lógicos representados en valores basados en cero.
258:259	Tamaño de granularidad de la prevención de errores de escritura del espacio de nombres (NTWPG). Este campo indica los incrementos de tamaño específicos del espacio de nombres por debajo de NTWPU de la operación de escritura garantizada que se escribirá atómicame nte en NVM durante un corte de corriente o una condición de error. Es decir, el tamaño debe ser NTWPG * n <= NTWPU, en el que n es entero positivo. El desplazamiento de LBA de la operación de escritura también debe estar alineado con este campo. Este campo se especifica en bloques lógicos representados en valores basados en cero.
260:263	Tamaño del límite de prevención de errores de escritura del espacio de nombres (NTWPB). Este campo indica el tamaño del límite atómico de este espacio de nombres para el valor NTWPU. No se garantiza que las escrituras en este espacio de nombres que sobrepasen los límites atómicos se escriban atómicamente en NVM durante un corte de corriente o una condición de error. Un valor de 0h indica que no hay límites atómicos para condiciones de corte de corriente o error. Todos

Bytes	Descripción
	los demás valores especifican un tamaño en términos de bloques lógicos mediante la misma codificación que el campo NTWPU.

Configurar la pila de software para la prevención de errores de escritura

La prevención de errores de escritura se activa de forma predeterminada en los tipos de instancia admitidos con volúmenes admitidos. No es necesario habilitar ninguna configuración adicional para habilitar el volumen o la instancia para la prevención de errores de escritura.

> **Note**
>
> No hay impacto en el rendimiento de las cargas de trabajo que no admiten la prevención de errores de escritura. No es necesario hacer ningún cambio para estas cargas de trabajo. Las cargas de trabajo que sí admiten la prevención de errores de escritura, pero que no están configuradas para utilizarla, siguen usando el búfer de doble escritura y no obtienen ninguna ventaja de rendimiento.

Para configurar la pila de software de MySQL o MariaDB con el fin de desactivar el búfer de doble escritura y utilizar la prevención de errores de escritura, complete los siguientes pasos:

1. Configure el volumen para utilizar el sistema de archivos ext4 con la opción BigAlloc y establezca el tamaño del clúster en 4 KiB, 8 KiB o 16 KiB. Usar BigAlloc con un tamaño de clúster de 4 KiB, 8 KiB o 16 KiB garantiza que el sistema de archivos asigne archivos que se alineen con el límite correspondiente.

   ```
   $  mkfs.ext4 -O bigalloc -C 4096|8192|16384 device_name
   ```

   > **Note**
   >
   > En MySQL y MariaDB, debe utilizar `-C 16384` para que coincida con el tamaño de página de base de datos. Establecer la granularidad de la asignación en un valor distinto de un múltiplo del tamaño de la página puede dar lugar a asignaciones que podrían

no coincidir con los límites de prevención de errores de escritura del dispositivo de almacenamiento.

Por ejemplo:

```
$  mkfs.ext4 -O bigalloc -C 16384 /dev/nvme1n1
```

2. Configure InnoDB para que utilice el método de vaciado `O_DIRECT` y desactive la doble escritura de InnoDB. Utilice su editor de texto preferido para abrir `/etc/my.cnf` y actualice los parámetros `innodb_flush_method` y `innodb_doublewrite` de la siguiente manera:

```
innodb_flush_method=O_DIRECT
innodb_doublewrite=0
```

Important

Si utiliza el administrador de volúmenes lógicos (LVM) u otra capa de virtualización de almacenamiento, asegúrese de que los desplazamientos iniciales de los volúmenes están alineados en múltiplos de 16 KiB. Esto es relativo al almacenamiento de NVMe subyacente para tener en cuenta las cabeceras de metadatos y los superbloques utilizados por la capa de virtualización de almacenamiento. Si se agrega un desplazamiento al volumen físico del LVM, puede provocar una falta de alineación entre las asignaciones del sistema de archivos y los desplazamientos del dispositivo de NVMe, lo que invalidaría la prevención de errores de escritura. Para obtener más información, consulte `--dataalignmentoffset` en la página del manual de Linux.

Recursos y etiquetas

Amazon EC2 proporciona distintos recursos que puede crear y usar. Algunos de ellos incluyen imágenes, instancias, volúmenes e instantáneas. Cuando se crea un recurso, se le asigna un ID de recurso único.

Algunos recursos se pueden etiquetar con valores que le sirven de ayuda para organizarlos e identificarlos.

En los temas siguientes se describen los recursos y las etiquetas, y cómo trabajar con ellos.

Contenido

Papelera de reciclaje

La papelera de reciclaje es una característica de recuperación de datos que le permite restaurar instantáneas de Amazon EBS y AMI basadas en EBS que se han eliminado por accidente. Cuando se utiliza la papelera de reciclaje, si se eliminan recursos, estos se retienen en la papelera de reciclaje durante un periodo que usted especifique antes de eliminarse de forma permanente.

Puede restaurar un recurso desde la papelera de reciclaje en cualquier momento antes de que se venza su periodo de retención. Después de restaurar un recurso desde la papelera de reciclaje, este se quita de la papelera de reciclaje y puede utilizarse de la misma manera que utiliza cualquier otro recurso de ese tipo en su cuenta. Si el periodo de retención se vence y el recurso no se restaura, este se elimina de forma permanente de la papelera de reciclaje y ya no estará disponible para su recuperación.

El uso de la papelera de reciclaje ayuda a garantizar la continuidad de la empresa, ya que protege los datos empresariales esenciales contra la eliminación accidental.

Temas

¿Cómo funciona?

Para habilitar y utilizar la papelera de reciclaje, debe crear reglas de retención en las regiones de AWS en las que desea proteger los recursos. Las reglas de retención especifican los siguientes elementos:

- el tipo de recurso que desea proteger
- los recursos que desea retener en la papelera de reciclaje cuando se eliminan
- el periodo de retención durante el que se retendrán los recursos en la papelera de reciclaje antes de eliminarlos de forma permanente

Con la papelera de reciclaje, puede crear dos tipos de reglas de retención:

- Reglas de retención a nivel de etiqueta: una regla de retención a nivel de etiqueta utiliza etiquetas de recursos para identificar los recursos que se van a retener en la papelera de reciclaje. Para cada regla de retención, se especifica uno o varios pares de claves de etiqueta y valores. Los recursos del tipo especificado etiquetados con al menos uno de los pares de claves de etiqueta y valores especificados en la regla de retención se retienen de forma automática en la papelera de reciclaje al eliminarlos. Utilice este tipo de regla de retención si desea proteger recursos específicos de la cuenta en función de sus etiquetas.
- Reglas de retención a nivel de región: una regla de retención a nivel de región no tiene ninguna etiqueta de recurso especificada. Se aplica a todos los recursos del tipo especificado en la región

en la que se crea la regla, incluso si los recursos no están etiquetados. Utilice este tipo de regla de retención si desea proteger todos los recursos de un tipo específico en una región específica.

Mientras un recurso esté en la papelera de reciclaje, tendrá la capacidad de restaurarlo para utilizarlo en cualquier momento.

El recurso permanece en la papelera de reciclaje hasta que se produzca una de las siguientes situaciones:

- La restaura manualmente para utilizarla. Cuando restaura un recurso de la papelera de reciclaje, el recurso se elimina de la papelera de reciclaje y queda inmediatamente disponible para su uso. Puede utilizar los recursos restaurados de la misma manera que cualquier otro recurso de ese tipo en su cuenta.
- El periodo de retención se vence. Si el periodo de retención se vence y el recurso no se ha restaurado desde la papelera de reciclaje, el recurso se elimina de forma permanente de la papelera de reciclaje y ya no se puede ver ni restaurar.

Recursos admitidos

La papelera de reciclaje admite los siguientes tipos de recursos:

- Instantáneas de Amazon EBS

> **Important**
>
> Las reglas de retención de la papelera de reciclaje también se aplican a las instantáneas archivadas en el almacenamiento de archivos. Si elimina una instantánea archivada que coincide con una regla de retención, esa instantánea se retiene en la papelera de reciclaje durante el periodo definido en la regla de retención. Las instantáneas archivadas se facturan al precio de las instantáneas archivadas mientras se encuentran en la papelera de reciclaje.

- imágenes de máquina de Amazon (AMI) basadas en Amazon EBS

> **Note**
>
> Las reglas de retención también se aplican a las AMI deshabilitadas.

Consideraciones

Las siguientes consideraciones se aplican cuando se trabaja con la papelera de reciclaje y las reglas de retención.

Consideraciones generales

- **Important**

  Cuando crea la primera regla de retención, esta puede tardar hasta 30 minutos en activarse y comenzar a retener los recursos. Después de crear la primera regla de retención, las siguientes reglas de retención se activan y comienzan a retener los recursos casi de inmediato.

- Si un recurso coincide con más de una regla de retención tras su eliminación, prevalece la regla de retención con el periodo de retención más largo.
- No se puede eliminar un recurso de la papelera de reciclaje de forma manual. El recurso se eliminará de forma automática cuando venza el periodo de retención.
- Mientras haya un recurso en la papelera de reciclaje, solo podrá verlo, restaurarlo o modificar sus etiquetas. Para utilizar el recurso de cualquier otra forma, primero debe restaurarlo.
- Si algún Servicio de AWS, como AWS Backup o Amazon Data Lifecycle Manager, elimina un recurso que coincide con una regla de retención, la papelera de reciclaje retiene automáticamente ese recurso.
- Cuando se envía un recurso a la papelera de reciclaje, se asigna la siguiente etiqueta generada por el sistema al recurso:
  - Clave de etiqueta: `aws:recycle-bin:resource-in-bin`
  - Valor de etiqueta: `true`

  No puede editar ni eliminar esta etiqueta de forma manual. Cuando el recurso se restaura desde la papelera de reciclaje, la etiqueta se elimina de forma automática.

Consideraciones sobre las instantáneas

- **Important**

  Si tiene reglas de retención para las AMI y para las instantáneas asociadas, haga que el periodo de retención de las instantáneas sea igual o mayor que el periodo de retención de

las AMI. Esto garantiza que la papelera de reciclaje no elimine las instantáneas asociadas a una AMI antes de eliminar la propia AMI, ya que esto haría que la AMI no se pueda recuperar.

- Si una instantánea está habilitada para la restauración rápida de instantáneas cuando se elimina, la restauración rápida de instantáneas se desactiva automáticamente poco después de enviar la instantánea a la papelera de reciclaje.
  - Si restaura la instantánea antes de que se desactive la restauración rápida de instantáneas para la instantánea, esta última permanecerá habilitada.
  - Si restaura la instantánea, una vez desactivada la restauración rápida de instantáneas, esta última permanece como tal. Si es necesario, debe volver a habilitar manualmente la restauración rápida de instantáneas.
- Si se comparte una instantánea cuando se elimina, el uso compartido se anula de forma automática cuando se envía a la papelera de reciclaje. Si restaura la instantánea, todos los permisos de uso compartido anteriores se restauran automáticamente.
- Si una instantánea creada por otro servicio de AWS, como AWS Backup, se envía a la papelera de reciclaje y luego se restaura esa instantánea desde la papelera de reciclaje, el servicio de AWS que la creó ya no la administra. Debe eliminar la instantánea de forma manual si ya no se necesita.

Consideraciones sobre las AMI

- Solo se admiten las AMI basadas en Amazon EBS.
- **Important**

  Si tiene reglas de retención para las AMI y para las instantáneas asociadas, haga que el periodo de retención de las instantáneas sea igual o mayor que el periodo de retención de las AMI. Esto garantiza que la papelera de reciclaje no elimine las instantáneas asociadas a una AMI antes de eliminar la propia AMI, ya que esto haría que la AMI no se pueda recuperar.
- Si se comparte una AMI cuando se elimina, el uso compartido se anula de forma automática cuando se envía a la papelera de reciclaje. Si restaura la AMI, todos los permisos de uso compartido anteriores se restauran de forma automática.

- Antes de poder restaurar una AMI desde la papelera de reciclaje, primero debe restaurar todas las instantáneas asociadas desde la papelera de reciclaje y asegurarse de que se encuentran en el estado `available`.
- Si las instantáneas asociadas a la AMI se eliminan de la papelera de reciclaje, la AMI ya no se puede recuperar. La AMI se eliminará cuando venza el periodo de retención.
- Si una AMI creada por otro servicio de AWS, como AWS Backup, se envía a la papelera de reciclaje y luego se restaura esa AMI desde la papelera de reciclaje, el servicio de AWS que la creó ya no la administra. Debe eliminar la AMI de forma manual si ya no se necesita.

Consideraciones sobre las políticas de instantáneas de Amazon Data Lifecycle Manager

- Si Amazon Data Lifecycle Manager elimina una instantánea que coincide con una regla de retención, la papelera de reciclaje retiene automáticamente esa instantánea.
- Si Amazon Data Lifecycle Manager elimina una instantánea y la envía a la papelera de reciclaje cuando se alcanza el umbral de retención de la política y restaura manualmente la instantánea desde la papelera de reciclaje, debe eliminarla de forma manual cuando ya no sea necesaria. Amazon Data Lifecycle Manager dejará de administrar la instantánea.
- Si elimina manualmente una instantánea creada por una política y esa instantánea se encuentra en la papelera de reciclaje cuando se alcanza el umbral de retención de la política, Amazon Data Lifecycle Manager no eliminará la instantánea. Amazon Data Lifecycle Manager no administra instantáneas mientras se almacenan en la papelera de reciclaje.

  Si la instantánea se restaura desde la papelera de reciclaje antes de alcanzar el umbral de retención de la política, Amazon Data Lifecycle Manager eliminará la instantánea cuando se alcance el umbral de retención de la política.

  Si la instantánea se restaura desde la papelera de reciclaje una vez alcanzado el umbral de retención de la política, Amazon Data Lifecycle Manager ya no eliminará la instantánea. Debe eliminar manualmente la última instantánea cuando ya no la necesite.

Consideraciones sobre AWS Backup

- Si AWS Backup elimina una instantánea que coincide con una regla de retención, la papelera de reciclaje retiene automáticamente esa instantánea.

Consideraciones sobre las instantáneas archivadas

- Las reglas de retención de la papelera de reciclaje también se aplican a las instantáneas archivadas en el almacenamiento de archivos. Si elimina una instantánea archivada que coincide con una regla de retención, esa instantánea se retiene en la papelera de reciclaje durante el periodo definido en la regla de retención.

  Las instantáneas archivadas se facturan al precio de las instantáneas archivadas mientras se encuentran en la papelera de reciclaje.

  Si una regla de retención elimina una instantánea archivada de la papelera de reciclaje antes del periodo de archivado mínimo de 90 días, se facturarán los días restantes. Para obtener más información, consulte Precios y facturación de instantáneas archivadas en la Guía del usuario de Amazon EBS.

  Para utilizar una instantánea archivada de la papelera de reciclaje, primero debe recuperarla de la papelera de reciclaje y, luego, restaurarla del nivel de archivo al nivel estándar.

Cuotas

Las siguientes cuotas se aplican a la papelera de reciclaje.

Cuota	Cuota predeterminada			
Reglas de retención por región	250			
Pares de claves de etiquetas y valores por regla de retención	50			

Servicios relacionados

La papelera de reciclaje funciona con los siguientes servicios:

- AWS CloudTrail: permite registrar los eventos que se producen en la papelera de reciclaje. Para obtener más información, consulte Supervisar la papelera de reciclaje mediante AWS CloudTrail.

Precios

Los recursos de la papelera de reciclaje se facturan según las tarifas estándar. El uso de la papelera de reciclaje y las reglas de retención no tienen costos adicionales. Para obtener más información, consulte Precios Amazon EBS.

> **Note**
>
> Es posible que algunos recursos sigan apareciendo en la consola de la papelera de reciclaje o en la AWS CLI y la salida de la API durante un breve periodo después de que se hayan vencido los periodos de retención y se hayan eliminado de forma permanente. No se cobrarán estos recursos. La facturación se detiene en cuanto vence el periodo de retención.

Puede utilizar las siguientes etiquetas de asignación de costos generadas por AWS para fines de seguimiento y asignación de costos al utilizar AWS Billing and Cost Management.

- Clave: `aws:recycle-bin:resource-in-bin`
- Valor: `true`

Para más información, consulte Etiquetas de asignación de costos generadas por AWS en la Guía del usuario de AWS Billing and Cost Management.

Permisos de IAM necesarios

De forma predeterminada, los usuarios no tienen permiso para trabajar con la papelera de reciclaje, las reglas de retención ni los recursos que se encuentran en la papelera de reciclaje. Para permitir a los usuarios trabajar con estos recursos, debe crear políticas de IAM que concedan permisos para utilizar recursos específicos y acciones de la API. Una vez creadas las políticas, tendrá que agregar permisos a los usuarios, grupos o roles.

Temas

- Permisos para trabajar con la papelera de reciclaje y las reglas de retención
- Permisos para trabajar con los recursos de la papelera de reciclaje

- Claves de condición de la papelera de reciclaje

Permisos para trabajar con la papelera de reciclaje y las reglas de retención

Para trabajar con la papelera de reciclaje y las reglas de retención, los usuarios necesitan los siguientes permisos.

- `rbin:CreateRule`
- `rbin:UpdateRule`
- `rbin:GetRule`
- `rbin:ListRules`
- `rbin:DeleteRule`
- `rbin:TagResource`
- `rbin:UntagResource`
- `rbin:ListTagsForResource`
- `rbin:LockRule`
- `rbin:UnlockRule`

Para utilizar la consola de la papelera de reciclaje, los usuarios necesitan el permiso `tag:GetResources`.

A continuación, se muestra una política de IAM de ejemplo que incluye el permiso `tag:GetResources` para los usuarios de la consola. Si algunos permisos no se necesitan, puede eliminarlos de la política.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "rbin:CreateRule",
            "rbin:UpdateRule",
            "rbin:GetRule",
            "rbin:ListRules",
            "rbin:DeleteRule",
            "rbin:TagResource",
            "rbin:UntagResource",
```

```
            "rbin:ListTagsForResource",
            "rbin:LockRule",
            "rbin:UnlockRule",
            "tag:GetResources"
        ],
        "Resource": "*"
    }]
}
```

Para dar acceso, agregue permisos a los usuarios, grupos o roles:

- Usuarios y grupos en AWS IAM Identity Center:

  Cree un conjunto de permisos. Siga las instrucciones de Creación de un conjunto de permisos en la Guía del usuario de AWS IAM Identity Center.
- Usuarios administrados en IAM a través de un proveedor de identidades:

  Cree un rol para la federación de identidades. Siga las instrucciones descritas en Creación de un rol para un proveedor de identidad de terceros (federación) en la Guía del usuario de IAM.
- Usuarios de IAM:
  - Cree un rol que el usuario pueda aceptar. Siga las instrucciones descritas en Creación de un rol para un usuario de IAM en la Guía del usuario de IAM.
  - (No recomendado) Adjunte una política directamente a un usuario o añada un usuario a un grupo de usuarios. Siga las instrucciones descritas en Adición de permisos a un usuario (consola) de la Guía del usuario de IAM.

Permisos para trabajar con los recursos de la papelera de reciclaje

Para obtener más información sobre los permisos de IAM necesarios para trabajar con los recursos de la papelera de reciclaje, consulte lo siguiente:

- Permisos para trabajar con instantáneas en la papelera de reciclaje
- Permisos para trabajar con AMI en la papelera de reciclaje

Claves de condición de la papelera de reciclaje

La papelera de reciclaje define las siguientes claves de condición, que se pueden utilizar en el elemento `Condition` de una política de IAM para controlar las condiciones en las que se aplica la

declaración de la política. Para obtener más información, consulte Elementos de la política JSON de IAM: condición en la Guía del usuario de IAM.

Temas

- Clave de condición de rbin:Request/ResourceType
- Clave de condición de rbin:Attribute/ResourceType

Clave de condición de `rbin:Request/ResourceType`

La clave de condición `rbin:Request/ResourceType` se puede utilizar para filtrar el acceso en las solicitudes CreateRule y ListRules basadas en el valor especificado para el parámetro de solicitud `ResourceType`.

Ejemplo 1: CreateRule

El siguiente ejemplo de política de IAM permite a las entidades principales de IAM presentar solicitudes CreateRule solo si el valor especificado para el parámetro de solicitud `ResourceType` es `EBS_SNAPSHOT` o `EC2_IMAGE`. Esto permite a la entidad principal crear nuevas reglas de retención para instantáneas y AMI únicamente.

```
{
    "Version" : "2012-10-17",
    "Statement" : [
        {
            "Effect" : "Allow",
            "Action" :[
                "rbin:CreateRule"
            ],
            "Resource" : "*",
            "Condition" : {
                "StringEquals" : {
                    "rbin:Request/ResourceType" : ["EBS_SNAPSHOT", "EC2_IMAGE"]
                }
            }
        }
    ]
}
```

Ejemplo 2: ListRules

El siguiente ejemplo de política de IAM permite a las entidades principales de IAM presentar solicitudes ListRules solo si el valor especificado para el parámetro de solicitud `ResourceType` es `EBS_SNAPSHOT`. Esto permite que la entidad principal muestre las reglas de retención solo para instantáneas e impide que muestre las reglas de retención para cualquier otro tipo de recurso.

```
{
    "Version" : "2012-10-17",
    "Statement" : [
        {
            "Effect" : "Allow",
            "Action" :[
                "rbin:ListRules"
            ],
            "Resource" : "*",
            "Condition" : {
                "StringEquals" : {
                    "rbin:Request/ResourceType" : "EBS_SNAPSHOT"
                }
            }
        }
    ]
}
```

Clave de condición de **`rbin:Attribute/ResourceType`**

La clave de condición `rbin:Attribute/ResourceType` se puede utilizar para filtrar el acceso a las solicitudes DeleteRule, GetRule, UpdateRule, LockRule, UnlockRule, TagResource, UntagResource y ListTagsForResource basadas en el valor del atributo `ResourceType` de la regla de retención.

Ejemplo 1: UpdateRule

El siguiente ejemplo de política de IAM permite que las entidades principales de IAM realicen solicitudes UpdateRule solo si el atributo `ResourceType` de la regla de retención solicitada es `EBS_SNAPSHOT` o `EC2_IMAGE`. Esto permite a la entidad principal actualizar las reglas de retención para instantáneas y AMI únicamente.

```
{
    "Version" : "2012-10-17",
    "Statement" : [
        {
```

```
            "Effect" : "Allow",
            "Action" :[
                "rbin:UpdateRule"
            ],
            "Resource" : "*",
            "Condition" : {
                "StringEquals" : {
                    "rbin:Attribute/ResourceType" : ["EBS_SNAPSHOT", "EC2_IMAGE"]
                }
            }
        }
    ]
}
```

Ejemplo 2: DeleteRule

El siguiente ejemplo de política de IAM permite que las entidades principales de IAM realicen solicitudes DeleteRule solo si el atributo `ResourceType` de la regla de retención solicitada es `EBS_SNAPSHOT`. Esto permite a la entidad principal eliminar las reglas de retención para instantáneas únicamente.

```
{
    "Version" : "2012-10-17",
    "Statement" : [
        {
            "Effect" : "Allow",
            "Action" :[
                "rbin:DeleteRule"
            ],
            "Resource" : "*",
            "Condition" : {
                "StringEquals" : {
                    "rbin:Attribute/ResourceType" : "EBS_SNAPSHOT"
                }
            }
        }
    ]
}
```

Trabajar con reglas de retención

Para habilitar y utilizar la papelera de reciclaje, debe crear reglas de retención en las regiones de AWS en las que desea proteger los recursos. Las reglas de retención especifican los siguientes elementos:

- el tipo de recurso que desea proteger
- los recursos que desea retener en la papelera de reciclaje cuando se eliminan
- el periodo de retención durante el que se retendrán los recursos en la papelera de reciclaje antes de eliminarlos de forma permanente

Con la papelera de reciclaje, puede crear dos tipos de reglas de retención:

- Reglas de retención a nivel de etiqueta: una regla de retención a nivel de etiqueta utiliza etiquetas de recursos para identificar los recursos que se van a retener en la papelera de reciclaje. Para cada regla de retención, se especifica uno o varios pares de claves de etiqueta y valores. Los recursos del tipo especificado etiquetados con al menos uno de los pares de claves de etiqueta y valores especificados en la regla de retención se retienen de forma automática en la papelera de reciclaje al eliminarlos. Utilice este tipo de regla de retención si desea proteger recursos específicos de la cuenta en función de sus etiquetas.
- Reglas de retención a nivel de región: una regla de retención a nivel de región no tiene ninguna etiqueta de recurso especificada. Se aplica a todos los recursos del tipo especificado en la región en la que se crea la regla, incluso si los recursos no están etiquetados. Utilice este tipo de regla de retención si desea proteger todos los recursos de un tipo específico en una región específica.

Después de crear una regla de retención, los recursos que coinciden con sus criterios se retienen de forma automática en la papelera de reciclaje durante el periodo de retención especificado luego de la eliminación.

Temas

- Reglas de retención de etiquetas
- Ver las etiquetas de una regla de retención
- Eliminar las etiquetas de las reglas de retención
- Eliminar reglas de retención de la papelera de reciclaje

Crear una regla de retención

Cuando cree una regla de retención, debe especificar los siguientes parámetros obligatorios:

- El tipo de recurso que debe proteger la regla de retención.
- Los recursos que debe proteger la regla de retención. Puede crear reglas de retención por etiqueta y región.
  - Para crear una regla de retención a nivel de etiqueta, especifique las etiquetas de recursos que identifican los recursos que se van a proteger. Puede especificar un máximo de 50 etiquetas para cada regla y agregar el mismo par clave-valor de etiqueta a un máximo de cinco reglas de retención.
  - Para crear una regla de retención a nivel de región, no especifique ningún par clave-valor de etiqueta. En este caso, todos los recursos del tipo especificado están protegidos.
- El periodo para retener los recursos en la papelera de reciclaje tras la eliminación. El periodo puede ser de hasta 1 año (365 días).

También puede especificar los siguientes parámetros opcionales:

- Un nombre opcional para la regla de retención. El nombre puede tener una longitud de hasta 255 caracteres.
- Una descripción opcional para la regla de retención. La descripción puede tener una longitud máxima de 255 caracteres.

> **Note**
>
> Le recomendamos que no incluya información de identificación personal, confidencial o sensible en la descripción de la regla de retención.

- Etiquetas de reglas de retención opcionales para ayudar a identificar y organizar las reglas de retención. Puede asignar hasta 50 etiquetas a cada regla.

Si lo desea, también puede bloquear las reglas de retención en el momento de su creación. Si bloquea una regla de retención en la creación, también debe especificar el periodo de retraso en el desbloqueo, que puede ser de 7 a 30 días. Las reglas de retención permanecen desbloqueadas de forma predeterminada a menos que las bloquee explícitamente.

Las reglas de retención solo funcionan en las regiones en las que se han creado. Si tiene la intención de utilizar la papelera de reciclaje en otras regiones, debe crear reglas de retención adicionales en esas regiones.

Puede crear una regla de retención para la papelera de reciclaje mediante uno de los siguientes métodos.

Recycle Bin console

Para crear una regla de retención

1. Abra la consola de la papelera de reciclaje en https://console.aws.amazon.com/rbin/home/.
2. En el panel de navegación, elija Retention rules (Reglas de retención) y, a continuación, Create retention rule (Crear regla de retención).
3. En la sección Rule details (Detalles de regla) haga lo siguiente:
   a. (Opcional) En Retention rule name (Nombre de la regla de retención), escriba un nombre descriptivo para la regla de retención.
   b. (Opcional) En Retention rule description (Descripción de la regla de retención), ingrese una breve descripción para la regla de retención.
4. En la sección Rule settings (Configuración de reglas), realice lo siguiente:
   a. En Resource type (Tipo de recurso), elija el tipo de recurso que desea que proteja la regla de retención. La regla de retención retendrá solo los recursos de este tipo en la papelera de reciclaje.
   b. Realice una de las siguientes acciones siguientes:
      - Para crear una regla de retención a nivel de región que coincida con todos los recursos del tipo especificado eliminados de la región, seleccione Apply to all resources (Aplicar a todos los recursos). La regla de retención retendrá todos los recursos del tipo especificado eliminados en la papelera de reciclaje al eliminarlos, incluso si los recursos no tienen etiquetas.

- Para crear una regla de retención a nivel de etiqueta, en Resource tags to match (Etiquetas de recursos para coincidir), ingrese los pares de claves de etiqueta y valores que se utilizarán para identificar los recursos del tipo especificado que se van a retener en la papelera de reciclaje. La regla de retención solo retendrá los recursos del tipo especificado que tengan al menos uno de los pares de claves de etiqueta y valores especificados.

c. En Retention period (Periodo de retención), ingrese la cantidad de días durante los que la regla de retención va a retener los recursos en la papelera de reciclaje.

5. (Opcional) Para bloquear la regla de retención, en Rule lock settings (Configuración de bloqueo de reglas), seleccione Lock (Bloquear) y, luego, en Unlock delay period (Periodo de retraso del desbloqueo), especifique el periodo de retraso de desbloqueo en días. No se puede modificar ni eliminar ninguna regla de retención bloqueada. Para modificar o eliminar la regla, primero debe desbloquearla y, luego, esperar a que venza el periodo de retraso de desbloqueo. Para obtener más información, consulte Bloquear reglas de retención

   Para dejar la regla de retención desbloqueada, en Rule lock settings (Configuración de bloqueo de reglas), mantenga seleccionada la opción Unlock (Desbloquear). Una regla de retención desbloqueada se puede modificar o eliminar en cualquier momento. Para obtener más información, consulte Desbloquear reglas de retención.

6. (Opcional) En la sección Tags (Etiquetas), haga lo siguiente:

   - Para etiquetar la regla con etiquetas personalizadas, elija Add tag (Agregar etiqueta) y, a continuación, ingrese el par de clave de etiqueta y valor.

7. Elija Create retention rule (Crear regla de retención).

AWS CLI

Para crear una regla de retención

Utilice el comando create-rule de la AWS CLI. En `--retention-period`, especifique el número de días que deben retenerse las instantáneas eliminadas en la papelera de reciclaje. En `--resource-type`, especifique `EBS_SNAPSHOT` para las instantáneas o `EC2_IMAGE` para las AMI. Para crear una regla de retención a nivel de etiqueta, en `--resource-tags`, especifique las etiquetas que se utilizarán con el fin de identificar las instantáneas que se van a retener. Para crear una regla de retención a nivel de región, omita `--resource-tags`. Para bloquear una regla de retención, incluya `--lock-configuration` y especifique el periodo de retraso de desbloqueo en días.

```
aws rbin create-rule \
--retention-period RetentionPeriodValue=number_of_days,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT|EC2_IMAGE \
--description "rule_description" \
--lock-configuration
 'UnlockDelay={UnlockDelayUnit=DAYS,UnlockDelayValue=unlock_delay_in_days}' \
--resource-tags ResourceTagKey=tag_key,ResourceTagValue=tag_value
```

Ejemplo 1

El siguiente comando de ejemplo crea una regla de retención de región desbloqueada que retiene todas las instantáneas eliminadas durante un periodo de 7 días.

```
aws rbin create-rule \
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT \
--description "Match all snapshots"
```

Ejemplo 2

El siguiente comando de ejemplo crea una regla a nivel de etiqueta que retiene las instantáneas eliminadas que están etiquetadas con `purpose=production` durante un periodo de 7 días.

```
aws rbin create-rule \
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT \
--description "Match snapshots with a specific tag" \
--resource-tags ResourceTagKey=purpose,ResourceTagValue=production
```

Ejemplo 3

El siguiente comando de ejemplo crea una regla de retención de región bloqueada que retiene todas las instantáneas eliminadas durante un periodo de 7 días. La regla de retención está bloqueada con un periodo de retraso de desbloqueo de 7 días.

```
aws rbin create-rule \
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT \
--description "Match all snapshots" \
--lock-configuration 'UnlockDelay={UnlockDelayUnit=DAYS,UnlockDelayValue=7}'
```

Ver las reglas de retención de la papelera de reciclaje

Puede ver las reglas de retención de la papelera de reciclaje mediante uno de los siguientes métodos.

Recycle Bin console

Para ver las reglas de retención

1. Abra la consola de la papelera de reciclaje en https://console.aws.amazon.com/rbin/home/.
2. En el panel de navegación, elija Retention rules (Reglas de retención).
3. La cuadrícula enumera todas las reglas de retención de la región seleccionada. Para obtener más información acerca de una regla de retención específica, selecciónela en la cuadrícula.

AWS CLI

Para ver todas las reglas de retención

Utilice el comando de la AWS CLI list-rules, y en `--resource-type`, especifique `EBS_SNAPSHOT` para las instantáneas o `EC2_IMAGE` para las AMI.

```
aws rbin list-rules --resource-type EBS_SNAPSHOT|EC2_IMAGE
```

Ejemplo

El siguiente comando de ejemplo proporciona una lista de todas las reglas de retención que retienen las instantáneas.

```
aws rbin list-rules --resource-type EBS_SNAPSHOT
```

Para ver información de una regla de retención específica

Utilice el comando get-rule de la AWS CLI.

```
aws rbin get-rule --identifier rule_ID
```

Ejemplo

El siguiente comando de ejemplo proporciona información sobre la regla de retención `pwxIkFcvge4`.

```
aws rbin get-rule --identifier pwxIkFcvge4
```

Actualizar reglas de retención

Puede actualizar la descripción, las etiquetas de recursos y el periodo de retención de una regla de retención desbloqueada en cualquier momento después de su creación. No puede actualizar el tipo de recurso de una regla de retención ni el periodo de retraso de desbloqueo, incluso si la regla de retención está desbloqueada.

No puede actualizar una regla de retención bloqueada de ninguna manera. Si necesita modificar una regla de retención bloqueada, primero debe desbloquearla y esperar a que venza el periodo de retraso de desbloqueo.

Si necesita modificar el periodo de retraso de desbloqueo de una regla de retención bloqueada, debe desbloquear la regla de retención y esperar a que venza el periodo de retraso de desbloqueo actual. Cuando el periodo de retraso de desbloqueo haya vencido, debe volver a bloquear la regla de retención y especificar el nuevo periodo de retraso de desbloqueo.

> **Note**
>
> Le recomendamos que no incluya información de identificación personal, confidencial o sensible en la descripción de la regla de retención.

Después de actualizar una regla de retención, los cambios solo se aplican a los recursos nuevos que retiene. Los cambios no afectan a los recursos enviados anteriormente a la papelera de reciclaje. Por ejemplo, si actualiza el periodo de retención de una regla de retención, durante el nuevo periodo de retención solo se retendrán las instantáneas que se eliminen después de la actualización. Las instantáneas que envió a la papelera de reciclaje antes de la actualización se retienen durante el periodo de retención anterior (antiguo).

Puede actualizar una regla de retención mediante uno de los siguientes métodos.

Recycle Bin console

Para actualizar una regla de retención

1. Abra la consola de la papelera de reciclaje en https://console.aws.amazon.com/rbin/home/.

2. En el panel de navegación, elija Retention rules (Reglas de retención).
3. En la cuadrícula, seleccione la regla de retención que desea actualizar y elija Actions (Acciones), Edit retention rule (Editar regla de retención).
4. En la sección Rule details (Detalles de regla), actualice Retention rule name (Nombre de la regla de retención) y Retention rule description (Descripción de regla de retención) según sea necesario.
5. En la sección Rule settings (Configuración de reglas), actualice Resource type (Tipo de recurso), Resource tags to match (Etiquetas de recursos para coincidir) y Retention period (Periodo de retención) según sea necesario.
6. En la sección Tags (Etiquetas), agregue o elimine etiquetas de reglas de retención según sea necesario.
7. Elija Save retention rule (Guardar regla de retención).

AWS CLI

Para actualizar una regla de retención

Utilice el comando update-rule de la AWS CLI. En `--identifier`, especifique el ID de la regla de retención que desea actualizar. En `--resource-types`, especifique `EBS_SNAPSHOT` para las instantáneas o `EC2_IMAGE` para las AMI.

```
aws rbin update-rule \
--identifier rule_ID \
--retention-period RetentionPeriodValue=number_of_days,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT|EC2_IMAGE \
--description "rule_description"
```

Ejemplo

El siguiente comando de ejemplo actualiza la regla de retención `6lsJ2Fa9nh9`para retener todas las instantáneas durante 7 días y actualiza su descripción.

```
aws rbin update-rule \
--identifier 6lsJ2Fa9nh9 \
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT \
--description "Retain for three weeks"
```

Bloquear reglas de retención

La papelera de reciclaje permite bloquear las reglas de retención regionales en cualquier momento.

> **Note**
>
> No puede bloquear las reglas de retención de etiqueta.

Las reglas de retención bloqueadas no se pueden modificar ni eliminar, ni siquiera pueden hacerlo los usuarios que tengan los permisos de IAM necesarios. Bloquee las reglas de retención para ayudar a protegerlas contra modificaciones y eliminaciones accidentales o malintencionadas.

Cuando se bloquea una regla de retención, debe especificar un periodo de retraso de desbloqueo. Este es el periodo de tiempo que debe esperar después de desbloquear la regla de retención para poder modificarla o eliminarla. No puede modificar ni eliminar la regla de retención durante el periodo de retraso de desbloqueo. Puede modificar o eliminar la regla de retención solo después de que haya vencido el periodo de retraso de desbloqueo.

No puede cambiar el periodo de retraso de desbloqueo después de bloquear la regla de retención. Si los permisos de su cuenta se han visto comprometidos, el periodo de retraso de desbloqueo le da tiempo adicional para detectar a las amenazas de seguridad y responder a ellas. La duración de este periodo debe ser superior al tiempo que tarde en identificar las vulneraciones de seguridad y responder a ellas. Para establecer la duración correcta, puede revisar los incidentes de seguridad anteriores y el tiempo necesario para identificar y solucionar una vulneración de la cuenta.

Le recomendamos que utilice las reglas de Amazon EventBridge para notificarle los cambios en el estado de bloqueo de las reglas de retención. Para obtener más información, consulte Supervisar la papelera de reciclaje con Amazon EventBridge.

Consideraciones

- Solo puede bloquear las reglas de retención de región.
- Puede bloquear una regla de retención desbloqueada en cualquier momento.
- El periodo de retraso de desbloqueo debe ser de 7 a 30 días.
- Puede volver a bloquear una regla de retención durante el periodo de retraso de desbloqueo. Al volver a bloquear la regla de retención, se restablece el periodo de retraso de desbloqueo.

Puede bloquear una regla de retención de región mediante uno de los métodos siguientes.

Recycle Bin console

Para bloquear una regla de retención

1. Abra la consola de la papelera de reciclaje en https://console.aws.amazon.com/rbin/home/
2. En el panel de navegación, elija Retention rules (Reglas de retención).
3. En la cuadrícula, seleccione la regla de retención desbloqueada que desea bloquear y elija Actions (Acciones), Edit retention rule lock (Editar bloqueo de regla de retención).
4. En la pantalla Edit retention rule lock (Editar bloqueo de regla de retención), seleccione Lock (Bloquear) y, a continuación, en Unlock delay period (Periodo de retraso del desbloqueo), especifique el periodo de retraso de desbloqueo en días.
5. Seleccione la casilla I acknowledge that locking the retention rule will prevent it from being modified or deleted (Reconozco que bloquear la regla de retención impedirá que se modifique o elimine) y, a continuación, elija Save (Guardar).

AWS CLI

Para bloquear una regla de retención desbloqueada

Utilice el comando lock-rule de la AWS CLI. En `--identifier`, especifique el ID de la regla de retención que desea bloquear. En `--lock-configuration`, especifique el periodo de retraso de desbloqueo en días.

```
aws rbin lock-rule \
--identifier rule_ID \
--lock-configuration
 'UnlockDelay={UnlockDelayUnit=DAYS,UnlockDelayValue=number_of_days}'
```

Ejemplo

El comando de ejemplo siguiente bloquea la regla de retención `6lsJ2Fa9nh9` y establece el periodo de retraso de desbloqueo en 15 días.

```
aws rbin lock-rule \
--identifier 6lsJ2Fa9nh9 \
--lock-configuration 'UnlockDelay={UnlockDelayUnit=DAYS,UnlockDelayValue=15}'
```

Desbloquear reglas de retención

No puede modificar ni eliminar una regla de retención bloqueada. Si necesita modificar una regla de retención bloqueada, primero debe desbloquearla. Una vez que haya desbloqueado la regla de retención, debe esperar a que venza el periodo de retraso de desbloqueo antes de modificarla o eliminarla. No puede modificar ni eliminar una regla de retención durante el periodo de retraso de desbloqueo.

Un usuario que tenga los permisos de IAM necesarios puede modificar y eliminar una regla de retención desbloqueada en cualquier momento. Dejar las reglas de retención desbloqueadas podría exponerlas a modificaciones y eliminaciones accidentales o malintencionadas.

Consideraciones

- Puede volver a bloquear una regla de retención durante el periodo de retraso de desbloqueo.
- Puede volver a bloquear una regla de retención después de que haya vencido el periodo de retraso de desbloqueo.
- No puede omitir el periodo de retraso de desbloqueo.
- No puede cambiar el periodo de retraso de desbloqueo después del bloqueo inicial.

Le recomendamos que utilice las reglas de Amazon EventBridge para notificarle los cambios en el estado de bloqueo de las reglas de retención. Para obtener más información, consulte Supervisar la papelera de reciclaje con Amazon EventBridge.

Puede desbloquear una regla de retención bloqueada por región mediante uno de los métodos siguientes.

Recycle Bin console

Para desbloquear una regla de retención

1. Abra la consola de la papelera de reciclaje en https://console.aws.amazon.com/rbin/home/
2. En el panel de navegación, elija Retention rules (Reglas de retención).
3. En la cuadrícula, seleccione la regla de retención bloqueada que desea desbloquear y elija Actions (Acciones), Edit retention rule lock (Editar bloqueo de regla de retención).
4. En la pantalla Edit retention rule lock (Editar bloqueo de regla de retención), elija Unlock (Desbloquear) y, a continuación, Save (Guardar).

AWS CLI

Para desbloquear una regla de retención bloqueada

Utilice el comando unlock-rule de la AWS CLI. En `--identifier`, especifique el ID de la regla de retención que desea desbloquear.

```
aws rbin unlock-rule \
--identifier rule_ID
```

Ejemplo

El comando de ejemplo siguiente desbloquea la regla de retención `6lsJ2Fa9nh9`

```
aws rbin unlock-rule \
--identifier 6lsJ2Fa9nh9
```

Reglas de retención de etiquetas

Puede asignar etiquetas personalizadas a las reglas de retención para clasificarlas de diversas maneras; por ejemplo, por finalidad, propietario o entorno. Esto lo ayuda a encontrar de forma eficaz una regla de retención específica en función de las etiquetas personalizadas que haya asignado.

Puede asignar una etiqueta a una regla de retención mediante uno de los siguientes métodos.

Recycle Bin console

Para etiquetar una regla de retención

1. Abra la consola de la papelera de reciclaje en https://console.aws.amazon.com/rbin/home/.
2. En el panel de navegación, elija Retention rules (Reglas de retención).
3. Seleccione la regla de retención que desea etiquetar, elija la pestaña Tags (Etiquetas) y, a continuación, elija Manage tags (Administrar etiquetas).
4. Seleccione Agregar etiqueta. En Key (Clave), ingrese la clave de etiqueta. En Value (Valor), ingrese el valor de la etiqueta.
5. Elija Save (Guardar).

AWS CLI

Para etiquetar una regla de retención

Utilice el comando tag-resource de la AWS CLI. En `--resource-arn`, especifique el nombre de recurso de Amazon (ARN) de la regla de retención que se va a etiquetar y, en `--tags`, especifique el par de clave de etiqueta y valor.

```
aws rbin tag-resource \
--resource-arn retention_rule_arn \
--tags key=tag_key,value=tag_value
```

Ejemplo

En el siguiente ejemplo, el comando etiqueta la regla de retención `arn:aws:rbin:us-east-1:123456789012:rule/n0oSBBtItF3` con la etiqueta `purpose=production`.

```
aws rbin tag-resource \
--resource-arn arn:aws:rbin:us-east-1:123456789012:rule/n0oSBBtItF3 \
--tags key=purpose,value=production
```

Ver las etiquetas de una regla de retención

Puede ver las etiquetas asignadas a una regla de retención mediante uno de los siguientes métodos.

Recycle Bin console

Para ver las etiquetas de una regla de retención

1. Abra la consola de la papelera de reciclaje en https://console.aws.amazon.com/rbin/home/.
2. En el panel de navegación, elija Retention rules (Reglas de retención).
3. Seleccione la regla de retención para la que desea ver las etiquetas y elija la pestaña Tags (Etiquetas).

AWS CLI

Para ver las etiquetas asignadas a una regla de retención

Utilice el comando list-tags-for-resource de la AWS CLI. En `--resource-arn`, especifique el ARN de la regla de retención.

```
aws rbin list-tags-for-resource \
--resource-arn retention_rule_arn
```

Ejemplo

El siguiente comando de ejemplo muestra las etiquetas de la regla de retención `arn:aws:rbin:us-east-1:123456789012:rule/n0oSBBtItF3`.

```
aws rbin list-tags-for-resource \
--resource-arn arn:aws:rbin:us-east-1:123456789012:rule/n0oSBBtItF3
```

Eliminar las etiquetas de las reglas de retención

Puede quitar las etiquetas de una regla de retención mediante uno de los siguientes métodos.

Recycle Bin console

Para eliminar una etiqueta de una regla de retención

1. Abra la consola de la papelera de reciclaje en https://console.aws.amazon.com/rbin/home/.
2. En el panel de navegación, elija Retention rules (Reglas de retención).
3. Seleccione la regla de retención de la que desea eliminar la etiqueta y elija la pestaña Tags (Etiquetas) y, a continuación, elija Manage tags (Administrar etiquetas).
4. Elija Remove (Eliminar) junto a la etiqueta que desea eliminar.
5. Elija Save (Guardar).

AWS CLI

Para eliminar una etiqueta de una regla de retención

Utilice el comando untag-resource de la AWS CLI. En `--resource-arn`, especifique el ARN de la regla de retención. En `--tagkeys`, especifique las claves de etiqueta de las etiquetas que desea quitar.

```
aws rbin untag-resource \
--resource-arn retention_rule_arn \
--tagkeys tag_key
```

Ejemplo

El siguiente comando de ejemplo elimina las etiquetas que tienen una clave de etiqueta `purpose` de la regla de retención `arn:aws:rbin:us-east-1:123456789012:rule/nOoSBBtItF3`.

```
aws rbin untag-resource \
--resource-arn arn:aws:rbin:us-east-1:123456789012:rule/nOoSBBtItF3 \
--tagkeys purpose
```

Eliminar reglas de retención de la papelera de reciclaje

Puede eliminar una regla de retención en cualquier momento. Cuando se elimina una regla de retención, ya no retiene recursos nuevos en la papelera de reciclaje después de eliminarlos. Los recursos que se hayan enviado a la papelera de reciclaje antes de que se eliminara la regla de retención seguirán reteniéndose en la papelera de reciclaje según el periodo de retención definido en dicha regla. Cuando se vence el periodo, el recurso se elimina de forma permanente de la papelera de reciclaje.

Puede eliminar una regla de retención mediante uno de los siguientes métodos.

Recycle Bin console

Para eliminar una regla de retención

1. Abra la consola de la papelera de reciclaje en https://console.aws.amazon.com/rbin/home/.
2. En el panel de navegación, elija Retention rules (Reglas de retención).
3. En la cuadrícula, seleccione la regla de retención que desea eliminar y elija Actions (Acciones), Delete retention rule (Eliminar regla de retención).
4. Cuando se le solicite, ingrese el mensaje de confirmación y elija Delete retention rule (Eliminar regla de retención).

AWS CLI

Para eliminar una regla de retención

Utilice el comando delete-rule de la AWS CLI. En `--identifier`, especifique el ID de la regla de retención que desea eliminar.

```
aws rbin delete-rule --identifier rule_ID
```

Ejemplo

El siguiente comando de ejemplo elimina la regla de retención `6lsJ2Fa9nh9`.

```
aws rbin delete-rule --identifier 6lsJ2Fa9nh9
```

Trabajar con los recursos de la papelera de reciclaje

La papelera de reciclaje admite los siguientes tipos de recursos:

- Instantáneas de Amazon EBS
- imágenes de máquina de Amazon (AMI) basadas en Amazon EBS

Tareas

- Recuperar instantáneas de la papelera de reciclaje
- Recuperar las AMI de la papelera de reciclaje

Recuperar instantáneas de la papelera de reciclaje

La papelera de reciclaje es una característica de recuperación de datos que le permite restaurar instantáneas de Amazon EBS y AMI basadas en EBS que se han eliminado por accidente. Cuando se utiliza la papelera de reciclaje, si se eliminan recursos, estos se retienen en la papelera de reciclaje durante un periodo que usted especifique antes de eliminarse de forma permanente.

Puede restaurar un recurso desde la papelera de reciclaje en cualquier momento antes de que se venza su periodo de retención. Después de restaurar un recurso desde la papelera de reciclaje, este se quita de la papelera de reciclaje y puede utilizarse de la misma manera que utiliza cualquier otro recurso de ese tipo en su cuenta. Si el periodo de retención se vence y el recurso no se restaura, este se elimina de forma permanente de la papelera de reciclaje y ya no estará disponible para su recuperación.

Las instantáneas de la papelera de reciclaje se facturan con la misma tarifa que las instantáneas normales de la cuenta. El uso de la papelera de reciclaje y las reglas de retención no tienen costos adicionales. Para obtener más información, consulte Precios Amazon EBS.

Para obtener más información, consulte Papelera de reciclaje.

Temas

- Permisos para trabajar con instantáneas en la papelera de reciclaje
- Ver instantáneas en la papelera de reciclaje
- Restaurar instantáneas desde la papelera de reciclaje

Permisos para trabajar con instantáneas en la papelera de reciclaje

De forma predeterminada, los usuarios no tienen permiso para trabajar con las instantáneas que se encuentran en la papelera de reciclaje. Para permitir a los usuarios trabajar con estos recursos, debe crear políticas de IAM que concedan permisos para utilizar recursos específicos y acciones de la API. Una vez creadas las políticas, tendrá que agregar permisos a los usuarios, grupos o roles.

Para ver y recuperar las instantáneas que se encuentran en la papelera de reciclaje, los usuarios deben tener los siguientes permisos:

- `ec2:ListSnapshotsInRecycleBin`
- `ec2:RestoreSnapshotFromRecycleBin`

Para administrar las etiquetas de las instantáneas que se encuentran en la papelera de reciclaje, los usuarios necesitan los siguientes permisos adicionales.

- `ec2:CreateTags`
- `ec2:DeleteTags`

Para utilizar la consola de la papelera de reciclaje, los usuarios necesitan el permiso `ec2:DescribeTags`.

A continuación, se muestra una política de IAM de ejemplo. Incluye el permiso `ec2:DescribeTags` para los usuarios de la consola y los permisos `ec2:CreateTags` y `ec2:DeleteTags` para administrar etiquetas. Si los permisos no se necesitan, puede eliminarlos de la política.

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
```

```
        "Effect": "Allow",
        "Action": [
            "ec2:ListSnapshotsInRecycleBin",
            "ec2:RestoreSnapshotFromRecycleBin"
        ],
        "Resource": "*"
      },
      {
        "Effect": "Allow",
        "Action": [
            "ec2:CreateTags",
            "ec2:DeleteTags",
            "ec2:DescribeTags"
        ],
        "Resource": "arn:aws:ec2:Region:account-id:snapshot/*"
      },

    ]
}
```

Para dar acceso, agregue permisos a los usuarios, grupos o roles:

- Usuarios y grupos en AWS IAM Identity Center:

  Cree un conjunto de permisos. Siga las instrucciones de Creación de un conjunto de permisos en la Guía del usuario de AWS IAM Identity Center.

- Usuarios administrados en IAM a través de un proveedor de identidades:

  Cree un rol para la federación de identidades. Siga las instrucciones descritas en Creación de un rol para un proveedor de identidad de terceros (federación) en la Guía del usuario de IAM.

- Usuarios de IAM:
  - Cree un rol que el usuario pueda aceptar. Siga las instrucciones descritas en Creación de un rol para un usuario de IAM en la Guía del usuario de IAM.
  - (No recomendado) Adjunte una política directamente a un usuario o añada un usuario a un grupo de usuarios. Siga las instrucciones descritas en Adición de permisos a un usuario (consola) de la Guía del usuario de IAM.

Para obtener más información acerca de los permisos que se necesitan para usar la papelera de reciclaje, consulte Permisos para trabajar con la papelera de reciclaje y las reglas de retención.

Ver instantáneas en la papelera de reciclaje

Mientras haya una instantánea en la papelera de reciclaje, podrá ver información limitada al respecto, que incluye:

- El ID de la instantánea.
- La descripción de la instantánea.
- El ID del volumen desde el que se creó la instantánea.
- La fecha y la hora en que se eliminó la instantánea e ingresó en la papelera de reciclaje.
- La fecha y la hora en que se vence el periodo de retención. La instantánea se eliminará de forma permanente de la papelera de reciclaje en este momento.

Puede ver las instantáneas en la papelera de reciclaje mediante uno de los siguientes métodos.

Recycle Bin console

Para ver las instantáneas en la papelera de reciclaje mediante la consola

1. Abra la consola de la papelera de reciclaje en https://console.aws.amazon.com/rbin/home/
2. En el panel de navegación, elija Recycle Bin (Papelera de reciclaje).
3. La cuadrícula enumera todas las instantáneas que se encuentran actualmente en la papelera de reciclaje. Para ver los detalles de una instantánea específica, selecciónela en la cuadrícula y elija Actions (Acciones), View details (Ver detalles).

AWS CLI

Para ver instantáneas en la papelera de reciclaje mediante la AWS CLI

Utilice el comando list-snapshots-in-recycle-bin de la AWS CLI. Incluya la opción `--snapshot-id` para ver una instantánea específica. U omita la opción `--snapshot-id` para ver todas las instantáneas en la papelera de reciclaje.

```
aws ec2 list-snapshots-in-recycle-bin --snapshot-id snapshot_id
```

Por ejemplo, el siguiente comando proporciona información acerca de la instantánea `snap-01234567890abcdef` en la papelera de reciclaje.

```
aws ec2 list-snapshots-in-recycle-bin --snapshot-id snap-01234567890abcdef
```

Ejemplo de salida:

```
{
    "SnapshotRecycleBinInfo": [
        {
            "Description": "Monthly data backup snapshot",
            "RecycleBinEnterTime": "2021-12-01T13:00:00.000Z",
            "RecycleBinExitTime": "2021-12-15T13:00:00.000Z",
            "VolumeId": "vol-abcdef09876543210",
            "SnapshotId": "snap-01234567890abcdef"
        }
    ]
}
```

Restaurar instantáneas desde la papelera de reciclaje

No puede utilizar una instantánea de ninguna manera mientras está en la papelera de reciclaje. Para utilizar la instantánea, primero debe restaurarla. Cuando restaura una instantánea desde la papelera de reciclaje, la instantánea está disponible inmediatamente para su uso y se quita de la papelera de reciclaje. Puede utilizar una instantánea restaurada de la misma manera en que utiliza cualquier otra instantánea de la cuenta.

Puede restaurar una instantánea desde la papelera de reciclaje mediante uno de los siguientes métodos.

Recycle Bin console

Para restaurar una instantánea desde la papelera de reciclaje mediante la consola

1. Abra la consola de la papelera de reciclaje en https://console.aws.amazon.com/rbin/home/
2. En el panel de navegación, elija Recycle Bin (Papelera de reciclaje).
3. La cuadrícula enumera todas las instantáneas que se encuentran actualmente en la papelera de reciclaje. Seleccione la instantánea que desea restaurar y elija Recover (Recuperar).
4. Cuando se le pregunte, elija Recover (Recuperar).

AWS CLI

Para restaurar una instantánea eliminada de la papelera de reciclaje mediante la AWS CLI

Utilice el comando restore-snapshot-from-recycle-bin de la AWS CLI. En `--snapshot-id`, especifique el ID de la instantánea que desea restaurar.

```
aws ec2 restore-snapshot-from-recycle-bin --snapshot-id snapshot_id
```

Por ejemplo, el siguiente comando restaura la instantánea `snap-01234567890abcdef` de la papelera de reciclaje.

```
aws ec2 restore-snapshot-from-recycle-bin --snapshot-id snap-01234567890abcdef
```

Ejemplo de salida:

```
{
    "SnapshotId": "snap-01234567890abcdef",
    "Description": "Monthly data backup snapshot",
    "Encrypted": false,
    "OwnerId": "111122223333",
    "Progress": "100%",
    "StartTime": "2021-12-01T13:00:00.000000+00:00",
    "State": "recovering",
    "VolumeId": "vol-ffffffff",
    "VolumeSize": 30
}
```

Recuperar las AMI de la papelera de reciclaje

La papelera de reciclaje es una característica de recuperación de datos que le permite restaurar instantáneas de Amazon EBS y AMI basadas en EBS que se han eliminado por accidente. Cuando se utiliza la papelera de reciclaje, si se eliminan recursos, estos se retienen en la papelera de reciclaje durante un periodo que usted especifique antes de eliminarse de forma permanente.

Puede restaurar un recurso desde la papelera de reciclaje en cualquier momento antes de que se venza su periodo de retención. Después de restaurar un recurso desde la papelera de reciclaje, este se quita de la papelera de reciclaje y puede utilizarse de la misma manera que utiliza cualquier otro recurso de ese tipo en su cuenta. Si el periodo de retención se vence y el recurso no se restaura,

este se elimina de forma permanente de la papelera de reciclaje y ya no estará disponible para su recuperación.

Las AMI de la papelera de reciclaje no generan ningún gasto adicional.

Para obtener más información, consulte Papelera de reciclaje.

Temas

- Permisos para trabajar con AMI en la papelera de reciclaje
- Ver las AMI que se encuentran en la papelera de reciclaje
- Restaurar las AMI desde la papelera de reciclaje

Permisos para trabajar con AMI en la papelera de reciclaje

De forma predeterminada, los usuarios no tienen permiso para trabajar con las AMI que se encuentran en la papelera de reciclaje. Para permitir a los usuarios trabajar con estos recursos, debe crear políticas de IAM que concedan permisos para utilizar recursos específicos y acciones de la API. Una vez creadas las políticas, tendrá que agregar permisos a los usuarios, grupos o roles.

Para ver y recuperar las AMI que se encuentran en la papelera de reciclaje, los usuarios deben tener los siguientes permisos:

- `ec2:ListImagesInRecycleBin`
- `ec2:RestoreImageFromRecycleBin`

Para administrar las etiquetas de las AMI que se encuentran en la papelera de reciclaje, los usuarios necesitan los siguientes permisos adicionales.

- `ec2:CreateTags`
- `ec2:DeleteTags`

Para utilizar la consola de la papelera de reciclaje, los usuarios necesitan el permiso `ec2:DescribeTags`.

A continuación, se muestra una política de IAM de ejemplo. Incluye el permiso `ec2:DescribeTags` para los usuarios de la consola y los permisos `ec2:CreateTags` y `ec2:DeleteTags` para administrar etiquetas. Si los permisos no se necesitan, puede eliminarlos de la política.

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
            "ec2:ListImagesInRecycleBin",
            "ec2:RestoreImageFromRecycleBin"
        ],
        "Resource": "*"
      },
      {
        "Effect": "Allow",
        "Action": [
            "ec2:CreateTags",
            "ec2:DeleteTags",
            "ec2:DescribeTags"
        ],
        "Resource": "arn:aws:ec2:Region::image/*"
      }
    ]
}
```

Para dar acceso, agregue permisos a los usuarios, grupos o roles:

- Usuarios y grupos en AWS IAM Identity Center:

  Cree un conjunto de permisos. Siga las instrucciones de Creación de un conjunto de permisos en la Guía del usuario de AWS IAM Identity Center.

- Usuarios administrados en IAM a través de un proveedor de identidades:

  Cree un rol para la federación de identidades. Siga las instrucciones descritas en Creación de un rol para un proveedor de identidad de terceros (federación) en la Guía del usuario de IAM.

- Usuarios de IAM:
  - Cree un rol que el usuario pueda aceptar. Siga las instrucciones descritas en Creación de un rol para un usuario de IAM en la Guía del usuario de IAM.
  - (No recomendado) Adjunte una política directamente a un usuario o añada un usuario a un grupo de usuarios. Siga las instrucciones descritas en Adición de permisos a un usuario (consola) de la Guía del usuario de IAM.

Para obtener más información acerca de los permisos que se necesitan para usar la papelera de reciclaje, consulte Permisos para trabajar con la papelera de reciclaje y las reglas de retención.

Ver las AMI que se encuentran en la papelera de reciclaje

Mientras una AMI se encuentre en la papelera de reciclaje, podrá ver información limitada sobre ella, incluido lo siguiente:

- El nombre, la descripción y el ID único de la AMI.
- La fecha y la hora en las que se eliminó la AMI e ingresó a la papelera de reciclaje.
- La fecha y la hora en que se vence el periodo de retención. La AMI se eliminará de forma permanente en este momento.

Puede ver las AMI que se encuentran en la papelera de reciclaje siguiendo alguno de los métodos que se indican a continuación.

Recycle Bin console

Para ver las AMI eliminadas en la papelera de reciclaje usando la consola

1. Abra la consola de la papelera de reciclaje en console.aws.amazon.com/rbin/home/.
2. En el panel de navegación, elija Recycle Bin (Papelera de reciclaje).
3. La cuadrícula enumera todos los recursos que se encuentran actualmente en la papelera de reciclaje. Para ver los detalles de una AMI específica, selecciónela en la cuadrícula y elija Actions (Acciones), View details (Ver detalles).

AWS CLI

Para ver las AMI eliminadas en la papelera de reciclaje usando la AWS CLI

Utilice el comando list-images-in-recycle-bin de la AWS CLI. Para ver AMI específicas, incluya la opción `--image-id` y especifique los ID de las AMI que desea ver. Puede especificar hasta 20 ID en una única solicitud.

Para ver todas las AMI que se encuentran en la papelera de reciclaje, omita la opción `--image-id`. Si no especifica un valor para `--max-items`, de forma predeterminada, el comando devolverá 1000 elementos por página. Para obtener más información, consulte Paginación en la Referencia de la API de Amazon EC2.

```
aws ec2 list-images-in-recycle-bin --image-id ami_id
```

Por ejemplo, el siguiente comando proporciona información acerca de la AMI `ami-01234567890abcdef` en la papelera de reciclaje.

```
aws ec2 list-images-in-recycle-bin --image-id ami-01234567890abcdef
```

Ejemplo de salida:

```
{
    "Images": [
        {
            "ImageId": "ami-0f740206c743d75df",
            "Name": "My AL2 AMI",
            "Description": "My Amazon Linux 2 AMI",
            "RecycleBinEnterTime": "2021-11-26T21:04:50+00:00",
            "RecycleBinExitTime": "2022-03-06T21:04:50+00:00"
        }
    ]
}
```

Important

Si aparece el siguiente error, es posible que tenga que actualizar su versión de la AWS CLI. Para obtener más información, consulte Errores: comandos no encontrados.

```
aws.exe: error: argument operation: Invalid choice, valid choices are: ...
```

Restaurar las AMI desde la papelera de reciclaje

No puede utilizar una AMI de ninguna manera mientras está en la papelera de reciclaje. Para utilizar la AMI, primero debe restaurarla. Cuando se restaura una AMI desde la papelera de reciclaje, la AMI queda disponible inmediatamente para su uso y se quita de la papelera de reciclaje. Puede utilizar una AMI restaurada de la misma manera que utiliza cualquier otra AMI de su cuenta.

Puede restaurar una AMI desde la papelera de reciclaje siguiendo alguno de los métodos que se indican a continuación.

Recycle Bin console

Para restaurar una AMI desde la papelera de reciclaje usando la consola

1. Abra la consola de la papelera de reciclaje en console.aws.amazon.com/rbin/home/.
2. En el panel de navegación, elija Recycle Bin (Papelera de reciclaje).
3. La cuadrícula enumera todos los recursos que se encuentran actualmente en la papelera de reciclaje. Seleccione la AMI que desea restaurar y elija Recover (Recuperar).
4. Cuando se le pregunte, elija Recover (Recuperar).

AWS CLI

Para restaurar una AMI eliminada desde la papelera de reciclaje usando la AWS CLI

Utilice el comando restore-image-from-recycle-bin de la AWS CLI. En `--image-id`, especifique el ID de la AMI que desea restaurar.

```
aws ec2 restore-image-from-recycle-bin --image-id ami_id
```

Por ejemplo, el siguiente comando restaura la AMI `ami-01234567890abcdef` desde la papelera de reciclaje.

```
aws ec2 restore-image-from-recycle-bin --image-id ami-01234567890abcdef
```

Si el comando se ejecuta correctamente, no devuelve ningún resultado.

> **Important**
>
> Si aparece el siguiente error, es posible que tenga que actualizar su versión de la AWS CLI. Para obtener más información, consulte Errores: comandos no encontrados.
>
> ```
> aws.exe: error: argument operation: Invalid choice, valid choices are: ...
> ```

Supervisar la papelera de reciclaje

Puede utilizar las siguientes características para supervisar la papelera de reciclaje.

Temas

Supervisar la papelera de reciclaje con Amazon EventBridge

La papelera de reciclaje envía los eventos a Amazon EventBridge para las acciones hechas en las reglas de retención. Con EventBridge, puede establecer reglas que inicien acciones programáticas en respuesta a estos eventos. Por ejemplo, puede crear una regla de EventBridge que envíe una notificación a su correo electrónico cuando se desbloquee una regla de retención y entre en su periodo de retraso de desbloqueo. Para más información, consulte Creating Amazon EventBridge rules that react to events (Creación de reglas de Amazon EventBridge que reaccionan a los eventos).

Los eventos en EventBridge se representan como objetos JSON. Los campos únicos del evento se encuentran en la sección `detail` del objeto JSON. El campo `event` contiene el nombre del evento. El campo `result` contiene el estado completado de la acción que inició el evento. Para obtener más información, consulte Amazon EventBridge event patterns (Patrones de eventos de Amazon EventBridge) en la Guía del usuario de Amazon EventBridge.

Para más información acerca de Amazon EventBridge, consulte What Is Amazon EventBridge? (¿Qué es Amazon EventBridge?) en la Guía del usuario de Amazon EventBridge.

Eventos

- RuleLocked
- RuleChangeAttempted
- RuleUnlockScheduled
- RuleUnlockingNotice
- RuleUnlocked

RuleLocked

Este es un ejemplo de un evento que genera la papelera de reciclaje cuando una regla de retención se bloquea correctamente. Este evento se puede generar mediante las solicitudes CreateRule y LockRule. La API que generó el evento se indica en el campo `api-name`.

```
{
```

```
  "version": "0",
  "id": "exampleb-b491-4cf7-a9f1-bf370example",
  "detail-type": "Recycle Bin Rule Locked",
  "source": "aws.rbin",
  "account": "123456789012",
  "time": "2022-08-10T16:37:50Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
  ],
  "detail":
  {
    "detail-version": " 1.0.0",
    "rule-id": "a12345abcde",
    "rule-description": "locked account level rule",
    "unlock-delay-period": "30 days",
    "api-name": "CreateRule"
  }
}
```

RuleChangeAttempted

Este es un ejemplo de un evento que genera la papelera de reciclaje cuando se intenta modificar o eliminar una regla bloqueada incorrectamente. Este evento se puede generar mediante las solicitudes DeleteRule y UpdateRule. La API que generó el evento se indica en el campo `api-name`.

```
{
  "version": "0",
  "id": "exampleb-b491-4cf7-a9f1-bf370example",
  "detail-type": "Recycle Bin Rule Change Attempted",
  "source": "aws.rbin",
  "account": "123456789012",
  "time": "2022-08-10T16:37:50Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
  ],
  "detail":
  {
    "detail-version": " 1.0.0",
    "rule-id": "a12345abcde",
    "rule-description": "locked account level rule",
    "unlock-delay-period": "30 days",
```

```
    "api-name": "DeleteRule"
  }
}
```

RuleUnlockScheduled

Este es un ejemplo de un evento que genera la papelera de reciclaje cuando se desbloquea una regla de retención y comienza su periodo de retraso de desbloqueo.

```
{
  "version": "0",
  "id": "exampleb-b491-4cf7-a9f1-bf370example",
  "detail-type": "Recycle Bin Rule Unlock Scheduled",
  "source": "aws.rbin",
  "account": "123456789012",
  "time": "2022-08-10T16:37:50Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
  ],
  "detail":
  {
    "detail-version": " 1.0.0",
    "rule-id": "a12345abcde",
    "rule-description": "locked account level rule",
    "unlock-delay-period": "30 days",
    "scheduled-unlock-time": "2022-09-10T16:37:50Z",
  }
}
```

RuleUnlockingNotice

Este es un ejemplo de un evento que la papelera de reciclaje genera a diario mientras una regla de retención se encuentra en su periodo de retraso de desbloqueo, hasta el día antes de que venza el periodo de retraso de desbloqueo.

```
{
  "version": "0",
  "id": "exampleb-b491-4cf7-a9f1-bf370example",
  "detail-type": "Recycle Bin Rule Unlocking Notice",
  "source": "aws.rbin",
  "account": "123456789012",
```

```
  "time": "2022-08-10T16:37:50Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
  ],
  "detail":
  {
    "detail-version": " 1.0.0",
    "rule-id": "a12345abcde",
    "rule-description": "locked account level rule",
    "unlock-delay-period": "30 days",
    "scheduled-unlock-time": "2022-09-10T16:37:50Z"
  }
}
```

RuleUnlocked

Este es un ejemplo de un evento que genera la papelera de reciclaje cuando vence el periodo de retraso de desbloqueo de una regla de retención y la regla de retención se puede modificar o eliminar.

```
{
  "version": "0",
  "id": "exampleb-b491-4cf7-a9f1-bf370example",
  "detail-type": "Recycle Bin Rule Unlocked",
  "source": "aws.rbin",
  "account": "123456789012",
  "time": "2022-08-10T16:37:50Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
  ],
  "detail":
  {
    "detail-version": " 1.0.0",
    "rule-id": "a12345abcde",
    "rule-description": "locked account level rule",
    "unlock-delay-period": "30 days",
    "scheduled-unlock-time": "2022-09-10T16:37:50Z"
  }
}
```

Supervisar la papelera de reciclaje mediante AWS CloudTrail

El servicio de la papelera de reciclaje está integrado con AWS CloudTrail. CloudTrail es un servicio que proporciona un registro de las acciones que realiza un usuario, un rol o un servicio de AWS. CloudTrail captura como eventos todas las llamadas a la API realizadas en la papelera de reciclaje. Si crea un registro de seguimiento, puede habilitar la entrega continua de los eventos de CloudTrail a un bucket de Amazon Simple Storage Service (Amazon S3). Si no configura un registro de seguimiento, puede ver los eventos de administración más recientes en Event history (Historial de eventos) en la consola de CloudTrail. Puede utilizar la información que recopila CloudTrail para determinar la solicitud que se envió a la papelera de reciclaje, la dirección IP desde la que se realizó la solicitud, quién realizó la solicitud, cuándo la realizó y detalles adicionales.

Para obtener más información acerca de CloudTrail, consulte la Guía del usuario de AWS CloudTrail.

Información de la papelera de reciclaje en CloudTrail

CloudTrail se habilita en su cuenta de AWS cuando la crea. Cuando se produce una actividad de eventos compatible en la papelera de reciclaje, la actividad se registra en un evento de CloudTrail junto con otros eventos de servicios de AWS en Event history (Historial de eventos). Puede ver, buscar y descargar los últimos eventos de la cuenta de AWS. Para obtener más información, consulte Visualización de eventos con el historial de eventos de CloudTrail.

Para mantener un registro continuo de los eventos en su cuenta de AWS, incluidos los eventos de la papelera de reciclaje, cree una traza. Un registro de seguimiento permite a CloudTrail que pueda enviar archivos de registro a un bucket de S3. De manera predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las regiones de AWS. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de S3 especificado. También es posible configurar otros servicios de AWS para analizar en profundidad y actuar en función de los datos de eventos recopilados en los registros de CloudTrail. Para obtener más información, consulte Información general acerca de la creación de una traza en la Guía del usuario de AWS CloudTrail.

Acciones de la API admitidas

En la papelera de reciclaje, puede utilizar CloudTrail para registrar las siguientes acciones de la API como los eventos de administración.

- CreateRule
- UpdateRule
- GetRules

- ListRule
- DeleteRule
- TagResource
- UntagResource
- ListTagsForResource
- LockRule
- UnlockRule

Para obtener más información sobre el registro de eventos de administración, consulte Registrar eventos de administración para seguimientos en la Guía del usuario de CloudTrail.

Información de identidad

Cada entrada de registro o evento contiene información acerca de quién generó la solicitud. La información de identidad del usuario lo ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales del usuario raíz o del usuario.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro servicio de AWS.

Para obtener más información, consulte userIdentityElement de CloudTrail.

Comprender las entradas del archivo de registro de la papelera de reciclaje

Un registro de seguimiento es una configuración que permite la entrega de eventos como archivos de log al bucket de S3 que se especifique. Los archivos log de CloudTrail pueden contener una o varias entradas de log. Un evento representa una solicitud específica realizada desde un origen cualquiera, y contiene información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. Los archivos de registro de CloudTrail no rastrean el orden en la pila de las llamadas públicas a la API, por lo que estas no aparecen en ningún orden específico.

A continuación, se muestran ejemplos de entradas de registro de CloudTrail.

CreateRule

```
{
  "eventVersion": "1.08",
```

```
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-02T21:43:38Z"
      }
    }
  },
  "eventTime": "2021-08-02T21:45:22Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "CreateRule",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.9 Python/3.6.14
Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
  "requestParameters": {
    "retentionPeriod": {
      "retentionPeriodValue": 7,
      "retentionPeriodUnit": "DAYS"
    },
    "description": "Match all snapshots",
    "resourceType": "EBS_SNAPSHOT"
  },
  "responseElements": {
    "identifier": "jkrnexample"
  },
  "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
  "eventID": "714fafex-2eam-42pl-913e-926d4example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
```

```
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```

GetRule

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-02T21:43:38Z"
      }
    }
  },
  "eventTime": "2021-08-02T21:45:33Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "GetRule",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.9 Python/3.6.14
 Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
  "requestParameters": {
    "identifier": "jkrnexample"
```

```
  },
  "responseElements": null,
  "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
  "eventID": "714fafex-2eam-42pl-913e-926d4example",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```

ListRules

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-02T21:43:38Z"
      }
    }
  },
  "eventTime": "2021-08-02T21:44:37Z",
  "eventSource": "rbin.amazonaws.com",
```

```
  "eventName": "ListRules",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.9 Python/3.6.14
 Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
  "requestParameters": {
    "resourceTags": [
      {
        "resourceTagKey": "test",
        "resourceTagValue": "test"
      }
    ]
  },
  "responseElements": null,
  "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
  "eventID": "714fafex-2eam-42pl-913e-926d4example",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```

UpdateRule

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
```

```
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-02T21:43:38Z"
      }
    }
  },
  "eventTime": "2021-08-02T21:46:03Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "UpdateRule",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.9 Python/3.6.14
 Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
  "requestParameters": {
    "identifier": "jkrnexample",
    "retentionPeriod": {
      "retentionPeriodValue": 365,
      "retentionPeriodUnit": "DAYS"
    },
    "description": "Match all snapshots",
    "resourceType": "EBS_SNAPSHOT"
  },
  "responseElements": null,
  "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
  "eventID": "714fafex-2eam-42pl-913e-926d4example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```

DeleteRule


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-02T21:43:38Z"
      }
    }
  },
  "eventTime": "2021-08-02T21:46:25Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "DeleteRule",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.9 Python/3.6.14
 Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
  "requestParameters": {
    "identifier": "jkrnexample"
  },
  "responseElements": null,
  "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
  "eventID": "714fafex-2eam-42pl-913e-926d4example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
```

```
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```

TagResource

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-10-22T21:38:34Z"
      }
    }
  },
  "eventTime": "2021-10-22T21:43:15Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "TagResource",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.26 Python/3.6.14
 Linux/4.9.273-0.1.ac.226.84.332.metal1.x86_64 botocore/1.21.26",
  "requestParameters": {
    "resourceArn": "arn:aws:rbin:us-west-2:123456789012:rule/ABCDEF01234",
    "tags": [
      {
        "key": "purpose",
```

```
        "value": "production"
      }
    ]
  },
  "responseElements": null,
  "requestID": "examplee-7962-49ec-8633-795efexample",
  "eventID": "example4-6826-4c0a-bdec-0bab1example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```

UntagResource

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-10-22T21:38:34Z"
      }
    }
```

```
  },
  "eventTime": "2021-10-22T21:44:16Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "UntagResource",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.26 Python/3.6.14
 Linux/4.9.273-0.1.ac.226.84.332.metal1.x86_64 botocore/1.21.26",
  "requestParameters": {
    "resourceArn": "arn:aws:rbin:us-west-2:123456789012:rule/ABCDEF01234",
    "tagKeys": [
      "purpose"
    ]
  },
  "responseElements": null,
  "requestID": "example7-6c1e-4f09-9e46-bb957example",
  "eventID": "example6-75ff-4c94-a1cd-4d5f5example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```

ListTagsForResource

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
```

```
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-10-22T21:38:34Z"
      }
    }
  },
  "eventTime": "2021-10-22T21:42:31Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "ListTagsForResource",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.26 Python/3.6.14
 Linux/4.9.273-0.1.ac.226.84.332.metal1.x86_64 botocore/1.21.26",
  "requestParameters": {
    "resourceArn": "arn:aws:rbin:us-west-2:123456789012:rule/ABCDEF01234"
  },
  "responseElements": null,
  "requestID": "example8-10c7-43d4-b147-3d9d9example",
  "eventID": "example2-24fc-4da7-a479-c9748example",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```


LockRule


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
```

```
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2022-10-25T00:45:11Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2022-10-25T00:45:19Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "LockRule",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "python-requests/2.25.1",
  "requestParameters": {
    "identifier": "jkrnexample",
    "lockConfiguration": {
      "unlockDelay": {
        "unlockDelayValue": 7,
        "unlockDelayUnit": "DAYS"
      }
    }
  },
  "responseElements": {
    "identifier": "jkrnexample",
    "description": "",
    "resourceType": "EBS_SNAPSHOT",
    "retentionPeriod": {
      "retentionPeriodValue": 7,
      "retentionPeriodUnit": "DAYS"
    },
    "resourceTags": [],
    "status": "available",
    "lockConfiguration": {
```

```
      "unlockDelay": {
        "unlockDelayValue": 7,
        "unlockDelayUnit": "DAYS"
      }
    },
    "lockState": "locked"
  },
  "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
  "eventID": "714fafex-2eam-42pl-913e-926d4example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```

UnlockRule

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2022-10-25T00:45:11Z",
        "mfaAuthenticated": "false"
```

```
      }
    }
  },
  "eventTime": "2022-10-25T00:46:17Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "UnlockRule",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "python-requests/2.25.1",
  "requestParameters": {
    "identifier": "jkrnexample"
  },
  "responseElements": {
    "identifier": "jkrnexample",
    "description": "",
    "resourceType": "EC2_IMAGE",
    "retentionPeriod": {
      "retentionPeriodValue": 7,
      "retentionPeriodUnit": "DAYS"
    },
    "resourceTags": [],
    "status": "available",
    "lockConfiguration": {
      "unlockDelay": {
        "unlockDelayValue": 7,
        "unlockDelayUnit": "DAYS"
      }
    },
    "lockState": "pending_unlock",
    "lockEndTime": "Nov 1, 2022, 12:46:17 AM"
  },
  "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
  "eventID": "714fafex-2eam-42pl-913e-926d4example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
```

```
}
```

Ubicaciones de los recursos

Los recursos de Amazon EC2 son específicos de la región de AWS o la zona de disponibilidad en la que residen.

Recurso	Tipo	Descripción
Identificadores de recursos de Amazon EC2	Regional	Cada identificador de recurso, como un ID de AMI, de instancia, de volumen de EBS o de instantánea de EBS, está vinculado a su región y solo puede usarse en la región en la que fue creado.
Nombres de recursos proporcionados por el usuario	Regional	Cada nombre de recurso, como un nombre de grupo de seguridad o un nombre de par de claves, está vinculado a su región y solo puede usarse en la región en la que fue creado. Aunque puede crear recursos con el mismo nombre en varias regiones, no están relacionados entre sí.
AMI	Regional	Una AMI está vinculada a la región donde se encuentran los archivos dentro de Amazon S3. Puede copiar una AMI de una región en otra. Para obtener más información, consulte Copiar una AMI.
Instantáneas de EBS	Regional	Una instantánea de EBS está vinculada a su región y solo puede utilizarse para crear volúmenes en la misma región. Puede copiar una instantánea de una región a otra.
Volúmenes de EBS	Zona de disponibilidad	Los volúmenes de Amazon EBS están vinculado s a una zona de disponibilidad y solo se pueden adjuntar a instancias de esa misma zona de disponibilidad.

Recurso	Tipo	Descripción
Direcciones IP elásticas	Regional	Una dirección IP elástica está vinculada a una región y solo puede asociarse a una instancia que esté en la misma región.
Instancias	Zona de disponibilidad	Una instancia está vinculada a la zona de disponibilidad en la que se lanzó. Ahora bien, su ID de instancia está vinculado a la región.
Pares de claves	Global o regional	Los pares de claves que crea con Amazon EC2 están vinculadas a la región en la que se crean. Puede crear un par de claves RSA propio y cargarlo en la región en la que desea usarlo; por tanto, puede hacer que el par de claves esté disponible globalmente si lo carga en cada región. Para obtener más información, consulte Pares de claves e instancias de Amazon EC2.
Grupos de seguridad	Regional	Una grupo de seguridad está vinculado a una región y solo puede asociarse a una instancia de la misma región. No puede habilitar una instancia para comunicarse con una instancia fuera de su región por medio de reglas de grupo de seguridad . El tráfico desde una instancia de otra región se considera ancho de banda WAN.

ID de recursos

Cuando se crean recursos, a cada uno se le asigna un ID de recurso único. Un ID de recurso adopta la forma de un identificador de recursos (como `snap` para instantáneas), seguido de un guion y una combinación única de letras y números.

Cada identificador de recurso, como un ID de AMI, de instancia, de volumen de EBS o de instantánea de EBS, está vinculado a su región y solo puede usarse en la región en la que fue creado.

Puede usar los ID de los recursos para buscarlos en la consola de Amazon EC2. Si está usando una herramienta de línea de comandos o la API de Amazon EC2 para trabajar con Amazon EC2, los ID de recurso se necesitan con algunos comandos. Por ejemplo, si utiliza los comandos stop-instances de la AWS CLI para parar una instancia, debe especificar el ID de la instancia en el comando.

Longitud del ID del recurso

Antes de enero de 2016, los identificadores que se asignaban cuando se creaban ciertos tipos de recursos nuevos tenían 8 caracteres después del guión (por ejemplo, i-1a2b3c4d). Entre enero de 2016 y junio de 2018, cambiamos los identificadores de estos tipos de recursos para que utilizaran 17 caracteres después del guión (por ejemplo, `i-1234567890abcdef0`). En función del momento en que se haya creado la cuenta, es posible que algunos de los recursos existentes tengan identificadores cortos. No obstante, los nuevos recursos recibirán los identificadores más largos.

Enumerar y filtrar los recursos

Puede usar la consola de Amazon EC2 para obtener una lista de algunos tipos de recursos. Puede obtener una lista de cada tipo de recurso mediante su correspondiente comando o acción de API. Si tiene muchos recursos, puede filtrar los resultados para incluir, o excluir, solo los recursos que coincidan con determinados criterios.

Contenido

Enumerar y filtrar recursos mediante la consola

Contenido

Enumerar recursos mediante la consola

Puede ver los tipos de recursos de Amazon EC2 más comunes mediante la consola. Para ver recursos adicionales, use la interfaz de línea de comandos o las acciones de API.

Para enumerar recursos de EC2 mediante la consola

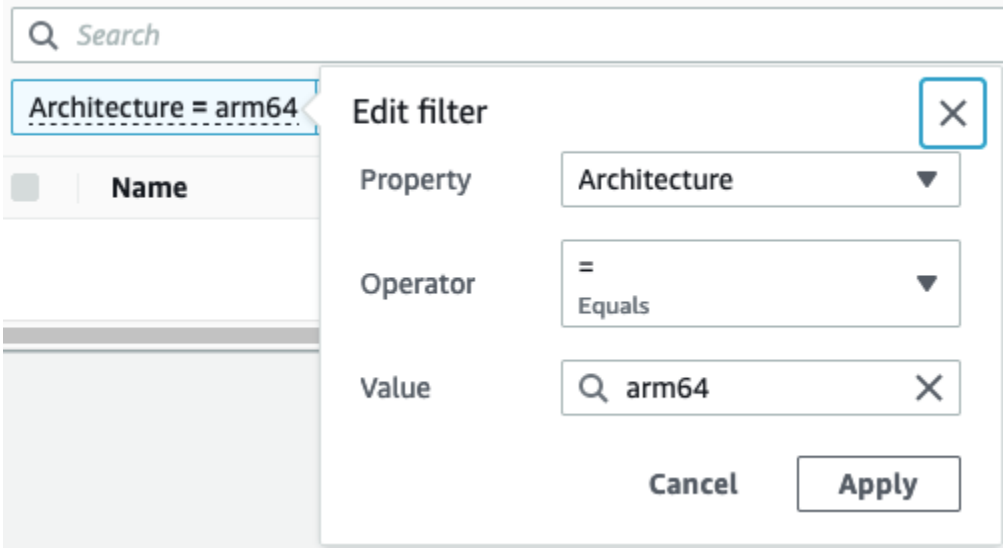
1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija la opción que corresponda al tipo de recurso. Por ejemplo, para enumerar las instancias, elija Instancias.

   La página muestra todos los recursos del tipo de recurso seleccionado.

Filtrar recursos mediante la consola

Para filtrar una lista de recursos

1. En el panel de navegación, seleccione un tipo de recurso (por ejemplo, Instances (Instancia[s])).
2. Elija el campo de búsqueda.
3. Seleccione el filtro en la lista.
4. Seleccione un operador; por ejemplo, = (igual que). Algunos atributos tienen más operadores disponibles para seleccionar. Tenga en cuenta que no todas las pantallas permiten seleccionar un operador.
5. Seleccione un valor de filtro.
6. Para editar un filtro seleccionado, elija el token del filtro (cuadro azul), realice las ediciones necesarias y luego elija Apply (Aplicar). Tenga en cuenta que no todas las pantallas permiten editar el filtro seleccionado.



7. Cuando haya terminado, quite el filtro.

Filtros compatibles

La consola de Amazon EC2 admite dos tipos de filtrado.

- El filtrado de API ocurre en el lado del servidor. El filtrado se aplica en la llamada a la API, lo que reduce el número de recursos devueltos por el servidor. Permite filtrar rápidamente entre grandes conjuntos de recursos, y puede reducir el tiempo de transferencia de datos y el costo entre el servidor y el navegador. El filtrado de API admite los operadores = (igual que) y : (contiene), y siempre distingue entre mayúsculas y minúsculas.
- El filtrado del cliente ocurre en el lado del cliente. Le permite filtrar los datos que ya están disponibles en el navegador (en otras palabras, los datos que ya han sido devueltos por la API). El filtrado de clientes funciona bien junto con un filtro API para filtrar a conjuntos de datos más pequeños en el navegador. Además de los operadores = (igual que) y : (contiene), el filtrado de clientes también puede admitir operadores de rangos, como >= (mayor o igual que), y de negación (inversos), como != (distinto de).

La consola de Amazon EC2 admite los siguientes tipos de búsquedas:

Buscar por palabra clave

La búsqueda por palabra clave es una búsqueda de texto libre que permite buscar un valor en la totalidad de los atributos o las etiquetas de los recursos, sin especificar una clave de atributo o etiqueta que se deba buscar.

> **Note**
>
> Todas las búsquedas de palabras clave utilizan el filtrado de clientes.

Para buscar por palabra clave, escriba o pegue lo que está buscando en el cuadro de búsqueda y, a continuación elija Entrar. Por ejemplo, buscar `123` devuelve todas las instancias que tengan 123 en cualquiera de sus atributos, como una dirección IP, un ID de instancia, un ID de VPC o un ID de AMI, o bien en cualquiera de sus etiquetas, como el nombre. Si la búsqueda de texto libre devuelve coincidencias inesperadas, aplique filtros adicionales.

Buscar por atributo

La búsqueda por un atributo le permite buscar un atributo específico en todos sus recursos.

> **Note**
>
> Las búsquedas de atributos utilizan filtrado de API o filtrado de clientes, según el atributo seleccionado. Al realizar una búsqueda de atributos, los atributos se agrupan en consecuencia.

Por ejemplo, puede buscar el atributo Instance State (Estado de la instancia) en todas las instancias para devolver solo las instancias que tienen el estado `stopped`. Para ello:

1. En el campo de búsqueda de la pantalla Instances (Instancia[s]), comience a escribir `Instance state`. A medida que escribe los caracteres, los dos tipos de filtros aparecen para el estado de instancia: filtros la API y filtros de cliente.
2. Para buscar en el lado del servidor, elija Instance state (Estado de la instancia) en los filtros de API. Para buscar en el lado del cliente, elija Instance state (client) (Estado de la instancia [cliente]) en los filtros de cliente.

   Aparecerá una lista de posibles operadores para el atributo seleccionado.
3. Elija el operador = (igual que).

   Aparecerá una lista de valores posibles para el atributo y el operador seleccionados.
4. Seleccione Stopped (Detenido) de la lista.

Buscar por etiqueta

La búsqueda por etiqueta permite filtrar los recursos de la tabla mostrada actualmente por una clave de etiqueta o un valor de etiqueta.

Las búsquedas de etiquetas utilizan filtrado de API o filtrado de clientes, en función de la configuración de la ventana Preferences (Preferencias).

Para garantizar el filtrado de API para etiquetas

1. Abra la ventana Preferences (Preferencias).
2. Desmarque la casilla de verificación Use regular expression matching (Utilizar coincidencia de expresiones regulares). Si esta casilla de verificación está seleccionada, se aplica filtrado de clientes.
3. Seleccione la casilla de verificación Use case sensitive matching (Utilizar coincidencia de mayúsculas y minúsculas). Si esta casilla de verificación no está marcada, se aplica filtrado de clientes.
4. Elija Confirmar.

Cuando se busca por etiqueta, se pueden utilizar los siguientes valores:

- (vacío): se buscan todos los recursos con la clave de etiqueta especificada, pero no debe haber ningún valor de etiqueta.
- All values (Todos los valores): se buscan todos los recursos con la clave de etiqueta especificada y cualquier valor de etiqueta.
- Not tagged (No etiquetado): se buscan todos los recursos que no tengan la clave de etiqueta especificada.
- Valor mostrado: se buscan todos los recursos con la clave de etiqueta especificada y el valor de etiqueta especificado.

Puede utilizar las siguientes técnicas para mejorar o refinar sus búsquedas.

Búsqueda inversa

Las búsquedas inversas permiten buscar recursos que no coinciden con un valor especificado. En las pantallas Instances (Instancia[s]) y AMIs (AMI), las búsquedas inversas se realizan seleccionando el operador != (distinto de) o !: (no contiene) y luego seleccionando un valor. En

otras pantallas, las búsquedas inversas se realizan anteponiendo el signo de exclamación de cierre (!) a la palabra clave de la búsqueda.

> **Note**
>
> La búsqueda inversa solo se admite con búsquedas de palabras clave y búsquedas de atributos en filtros de cliente. No se admite con búsquedas de atributos en filtros API.

Por ejemplo, puede buscar el atributo Instance State (Estado de la instancia) en todas las instancias para excluir todas las instancias que tengan el estado `terminated`. Para ello:

1. En el campo de búsqueda de la pantalla Instances (Instancia[s]), comience a escribir `Instance state`. A medida que escribe los caracteres, los dos tipos de filtros aparecen para el estado de instancia: filtros la API y filtros de cliente.
2. En Client filters (Filtros de cliente), elija Instance state (client) (Estado de la instancia [cliente]). La búsqueda inversa solo se admite en los filtros de cliente.

   Aparecerá una lista de posibles operadores para el atributo seleccionado.
3. Elija != (distinto de) y luego terminated (terminada).

Para filtrar instancias en función de un atributo de estado de la instancia, también puede utilizar los iconos de búsqueda (

) en la columna Instance state (Estado de la instancia). El icono de búsqueda con un signo más (+) muestra todas las instancias que coincidan con ese atributo. El icono de búsqueda con un signo menos (-) excluye todas las instancias que coincidan con ese atributo.

Otro ejemplo de uso de la búsqueda inversa: para ver una lista de todas las instancias que no tengan asignado el grupo de seguridad denominado `launch-wizard-1`, en Client filters (Filtros de cliente) busque por el atributo Security group name (Nombre del grupo de seguridad), elija != y, en la barra de búsqueda, ingrese `launch-wizard-1`.

Búsqueda parcial

Con búsquedas parciales, puede buscar valores de cadena parciales. Para realizar una búsqueda parcial, introduzca solo una parte de la palabra clave que desee buscar. En las pantallas Instances (Instancia[s]) y AMIs (AMI), las búsquedas parciales solo se pueden realizar con el operador : (contiene). En otras pantallas, se puede seleccionar el atributo de filtro de cliente e

ingresar inmediatamente solo una parte de la palabra clave que se desee buscar. Por ejemplo, en la pantalla Instance type (Tipo de instancia), para buscar todas las instancias `t2.micro`, `t2.small` y `t2.medium`, busque por el atributo Instance Type (Tipo de instancia) y, para la palabra clave, ingrese `t2`.

Búsqueda de expresiones regulares

Para utilizar búsquedas de expresiones regulares, se debe seleccionar la casilla de verificación Use regular expression matching (Utilizar coincidencia de expresiones regulares) en la ventana Preferences (Preferencias).

Las expresiones regulares resultan de utilidad cuando necesita que los valores en un campo coincidan con un determinado patrón. Por ejemplo, para buscar un valor que comience con `s`, busque `^s`. Para buscar un valor que termine con `xyz`, busque `xyz$`. O bien, para buscar un valor que comience con un número seguido de uno o más caracteres, busque `[0-9]+.*`.

> **Note**
>
> La búsqueda de expresiones regulares solo se admite con búsquedas de palabras clave y búsquedas de atributos en filtros de cliente. No se admite con búsquedas de atributos en filtros API.

Búsqueda distinguiendo entre mayúsculas y minúsculas

Para utilizar búsquedas que distingan entre mayúsculas y minúsculas, se debe seleccionar la casilla de verificación Use case sensitive matching (Utilizar coincidencia de mayúsculas y minúsculas) en la ventana Preferences (Preferencias). La preferencia de distinción entre mayúsculas y minúsculas solo se aplica a los filtros de cliente y de etiqueta.

> **Note**
>
> Los filtros de API siempre distinguen entre mayúsculas y minúsculas.

Búsqueda con comodín

Utilice el comodín `*` para que coincida con cero o más caracteres. Utilice el comodín `?` para que coincida con cero o un carácter. Por ejemplo, si tiene un conjunto de datos con los valores

`prod`, `prods` y`production`, buscar `prod*` devuelve todos los valores, mientras que `prod?` solo devuelve `prod` y `prods`. Para utilizar los valores literales, antepóngales una barra invertida (\) como carácter de escape. Por ejemplo, "`prod\*`" devolvería `prod*`.

> **Note**
>
> La búsqueda con comodín solo se admite en búsquedas de atributos y etiquetas en filtros de API. No se admite en búsquedas de palabras clave, ni en búsquedas de atributos y etiquetas en filtros de cliente.

Combinación de búsquedas

En general, se unen automáticamente varios filtros con el mismo atributo con `OR`. Por ejemplo, la búsqueda de `Instance State : Running` y `Instance State : Stopped` devuelve todas las instancias que se están ejecutando O detenidas. Para unir la búsqueda con `AND`, busque entre diferentes atributos. Por ejemplo, buscar `Instance State : Running` y `Instance Type : c4.large` devuelve solo instancias que son de tipo `c4.large` Y que están en el estado de ejecución.

Enumerar y filtrar mediante la CLI y la API

Cada tipo de recurso tiene un comando de CLI y una acción de API correspondiente que se usa para enumerar los recursos de ese tipo. Las listas de recursos resultantes pueden ser largas, por lo que puede ser más rápido y útil filtrar los resultados para incluir solo los recursos que coincidan con criterios específicos.

Consideraciones de filtrado

- Puede especificar hasta 50 filtros y hasta 200 valores por filtro en una única solicitud.
- Las cadenas de filtro pueden tener 255 caracteres como máximo.
- Puede utilizar comodines con los valores del filtro. Un asterisco (*) coincide con cero o con más caracteres y un signo de interrogación (?) coincide con cero o un carácter.
- Los valores de filtro distinguen entre mayúsculas y minúsculas.
- La búsqueda puede incluir los valores literales de los caracteres comodín; en ese caso, solo tiene que aplicarles escape con una barra oblicua inversa antes del carácter. Por ejemplo, un valor de `\*amazon\?\\` busca la cadena literal `*amazon?\`.

Filtros compatibles

Para ver los filtros compatibles para cada recurso de Amazon EC2, consulte la siguiente documentación:

- AWS CLI: Los comandos `describe` en la AWS CLI Command Reference de Amazon EC2.
- Tools for Windows PowerShell: Los comandos `Get` en la AWS Tools for PowerShell Cmdlet Reference de Amazon EC2.
- API de consulta: Las `Describe` acciones de API en la Referencia de la API de Amazon EC2.

Example Ejemplo: Especificar un filtro único

Puede enumerar sus instancias de Amazon EC2 mediante describe-instances. Sin filtros, la respuesta contiene información para todos los recursos. Puede utilizar el siguiente comando para incluir solo las instancias en ejecución en la salida.

```
aws ec2 describe-instances --filters Name=instance-state-name,Values=running
```

Para enumerar solo los ID de instancia de las instancias en ejecución, agregue el parámetro `--query` de la siguiente manera.

```
aws ec2 describe-instances --filters Name=instance-state-name,Values=running --query
 "Reservations[*].Instances[*].InstanceId" --output text
```

A continuación, se muestra un ejemplo del resultado.

```
i-0ef1f57f78d4775a4
i-0626d4edd54f1286d
i-04a636d18e83cfacb
```

Example Ejemplo: Especificar varios filtros o valores de filtro

Si especifica varios filtros o varios valores de filtro, el recurso debe coincidir con todos los filtros para incluirlos en los resultados.

Puede utilizar el siguiente comando para enumerar todas las instancias cuyo tipo es `m5.large` o `m5d.large`.

```
aws ec2 describe-instances --filters Name=instance-type,Values=m5.large,m5d.large
```

Puede utilizar el siguiente comando para enumerar todas las instancias detenidas cuyo tipo es `t2.micro`.

```
aws ec2 describe-instances --filters Name=instance-state-name,Values=stopped
 Name=instance-type,Values=t2.micro
```

Example Ejemplo: Usar comodines en un valor de filtro

Si especifica `database` como valor de filtro para el filtro `description` al describir las instantáneas de EBS mediante describe-snapshots, el comando devuelve solo las instantáneas cuya descripción es “database”.

```
aws ec2 describe-snapshots --filters Name=description,Values=database
```

El comodín * coincide con cero o más caracteres. Si especifica `*database*` como valor de filtro, el comando solo devuelve instantáneas cuya descripción incluye la base de datos de palabras.

```
aws ec2 describe-snapshots --filters Name=description,Values=*database*
```

El comodín ? coincide con exactamente 1 carácter. Si especifica `database?` como valor del filtro, el comando solo devuelve instantáneas cuya descripción es “database” o “database” seguido de un carácter.

```
aws ec2 describe-snapshots --filters Name=description,Values=database?
```

Si especifica `database????`, el comando solo devuelve instantáneas cuya descripción es “database” seguido de hasta cuatro caracteres. Excluye las descripciones con “database” seguido de cinco o más caracteres.

```
aws ec2 describe-snapshots --filters Name=description,Values=database????
```

Example Ejemplo: Filtro basado en la fecha

Con la AWS CLI, puede usar JMESPath para filtrar los resultados mediante expresiones. Por ejemplo, el siguiente comando describe-snapshots muestra los ID de todas las instantáneas creadas por su Cuenta de AWS (representada por *`123456789012`*) antes de la fecha especificada (representada por *`31/03/2020`*). Si no especifica el propietario, los resultados incluyen todas las instantáneas públicas.

```
aws ec2 describe-snapshots --filters Name=owner-id,Values=123456789012 --query
 "Snapshots[?(StartTime<='2020-03-31')].[SnapshotId]" --output text
```

El siguiente comando muestra los ID de todas las instantáneas creadas en el intervalo de fechas especificado.

```
aws ec2 describe-snapshots --filters Name=owner-id,Values=123456789012 --query
 "Snapshots[?(StartTime>='2019-01-01') && (StartTime<='2019-12-31')].[SnapshotId]" --
output text
```

Filtro basado en etiquetas

Para obtener ejemplos de cómo filtrar una lista de recursos según sus etiquetas, consulte Trabajar con etiquetas mediante la línea de comandos.

Visualización de recursos entre regiones mediante Amazon EC2 Global View

Amazon EC2 Global View permite ver y buscar recursos de Amazon EC2 y Amazon VPC en una sola región de AWS o en varias regiones simultáneamente en una sola consola. Para obtener más información, consulte Amazon EC2 Global View.

Amazon EC2 Global View

Amazon EC2 Global View permite ver algunos de sus recursos de Amazon EC2 y Amazon VPC en una sola región de AWS o a través de varias regiones en una sola consola. Amazon EC2 Global View también ofrece la funcionalidad de búsqueda global que permite buscar recursos específicos o tipos de recursos específicos en varias regiones simultáneamente.

Amazon EC2 Global View no permite modificar recursos de ninguna manera.

Recursos admitidos

Con Amazon EC2 Global View, puede ver un resumen global de los siguientes recursos en todas las regiones para las que su Cuenta de AWS está habilitada.

- Grupos de escalado automático
- Conjunto de opciones de DHCP

- Puerta de enlace de Internet de solo salida
- Direcciones IP elásticas
- Servicios de punto de conexión
- instancias
- Gateways de Internet
- Listas de prefijos administradas
- Puerta de enlace de NAT
- ACL de red
- Interfaces de red
- Tablas de enrutamiento
- Grupos de seguridad
- Subredes
- Volúmenes
- VPC
- Puntos de conexión de VPC
- Interconexiones de VPC

Permisos necesarios

Un usuario debe contar con los siguientes permisos para utilizar Amazon EC2 Global View.

```
{
  "Version": "2012-10-17",
  "Statement": [
  {
    "Effect": "Allow",
    "Action": [
    "autoscaling:DescribeAutoScalingGroups",
    "ec2:DescribeRegions",
    "ec2:DescribeDhcpOptions",
    "ec2:DescribeEgressOnlyInternetGateways",
    "ec2:DescribeAddresses",
    "ec2:DescribeVpcEndpointServices",
    "ec2:DescribeInstances",
    "ec2:DescribeInternetGateways",
    "ec2:DescribePrefixLists",
```

```
    "ec2:DescribeNatGateways",
    "ec2:DescribeNetworkAcls",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVolumes",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcPeeringConnections"
  ],
  "Resource": "*"
  }]
}
```

Para utilizar Amazon EC2 Global View

Abra la consola de Amazon EC2 Global View en https://console.aws.amazon.com/ec2globalview/home.

> **Important**
>
> No puede utilizar una ventana privada en Firefox para acceder a Amazon EC2 Global View.

La consola consta de lo siguiente:

- Region explorer (Explorador de regiones): esta pestaña incluye las siguientes secciones:
  - Resumen: se proporciona información general de alto nivel de los recursos de todas las regiones.

    Regiones habilitadas indica el número de regiones para las que se encuentra habilitada su Cuenta de AWS. Los campos restantes indican el número de recursos que tiene actualmente en esas regiones. Elija cualquiera de los enlaces para ver los recursos de ese tipo en todas las regiones. Por ejemplo, si el enlace debajo de la etiqueta Instances (Instancia[s]) es 29 de 10 regiones, indica que actualmente tiene 29 instancias en 10 regiones. Elija el enlace para ver una lista de las 29 instancias.
  - Recuentos de regiones de recursos: enumera todas las Regiones de AWS (incluidas aquellas para las que no se encuentra habilitada su cuenta) y proporciona totales para cada tipo de recurso para cada región.

Elija el nombre de una región para ver todos los recursos de todos los tipos de esa región específica. Por ejemplo, elija África (Ciudad del Cabo) af-south-1 para ver todas las VPC, subredes, instancias, grupos de seguridad, volúmenes y grupos de escalado automático de esa región. También puede seleccionar una región y elegir View resources for selected Region (Ver recursos para la región seleccionada).

Elija el valor de un tipo de recurso específico en una región específica para solo ver los recursos de ese tipo en esa región. Por ejemplo, elija el valor de instancias para África (Ciudad del Cabo) af-south-1 a fin de ver solo las instancias de esa región.

- Global search (Búsqueda global): esta pestaña permite buscar recursos específicos o tipos de recursos específicos en una sola región o en varias regiones. También permite ver los detalles de un recurso específico.

  Para buscar recursos, ingrese los criterios de búsqueda en el campo que precede a la cuadrícula. Puede buscar por región, tipo de recurso y las etiquetas asignadas a los recursos.

  Para consultar los detalles de un recurso específico, selecciónelo en la cuadrícula. También puede elegir el ID de recurso de un recurso para abrirlo en su respectiva consola. Por ejemplo, elija un ID de instancia para abrir la instancia en la consola de Amazon EC2 o elija un ID de subred a fin de abrir la subred en la consola de Amazon VPC.

> **Tip**
>
> Si solo usa regiones o tipos de recursos específicos, puede personalizar Amazon EC2 Global View para mostrar solo esas regiones y tipos de recursos. Para personalizar las regiones y los tipos de recursos que se muestran, en el panel de navegación, seleccione Configuración y, a continuación, en las pestañas Recursos y Regiones, seleccione las regiones y los tipos de recursos que no desee que se muestren en Amazon EC2 Global View.

Etiquetar los recursos de Amazon EC2

Para ayudarle a administrar las instancias, imágenes y otros recursos de Amazon EC2, puede asignar sus propios metadatos a cada recurso en forma de etiquetas. Las etiquetas le permiten clasificar los recursos de AWS de diversas maneras, por ejemplo, según su finalidad, propietario o entorno. Esto es útil cuando tiene muchos recursos del mismo tipo: puede identificar rápidamente un

recurso específico en función de las etiquetas que le haya asignado. En este tema se describe qué son las etiquetas y cómo crearlas.

> **Warning**
>
> Las claves de etiqueta y sus valores se devuelven mediante muchas llamadas a API diferentes. Denegar el acceso a `DescribeTags` no deniega automáticamente el acceso a etiquetas devueltas por otras API. Como práctica recomendada, no debe incluir datos confidenciales en las etiquetas.

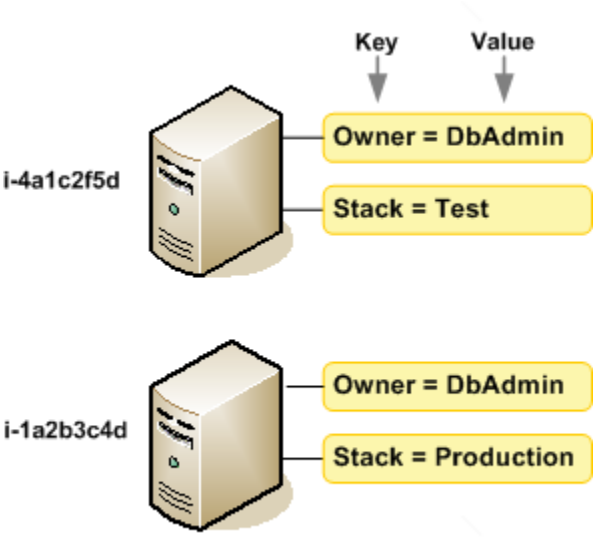
Contenido

Conceptos básicos de etiquetas

Una etiqueta es una marca que se asigna a un recurso de AWS. Cada etiqueta está formada por una clave y un valor opcional, ambos definidos por el usuario.

Las etiquetas le permiten clasificar los recursos de AWS de diversas maneras, por ejemplo, según su finalidad, propietario o entorno. Por ejemplo, podría definir un conjunto de etiquetas para las instancias Amazon EC2 de su cuenta que le ayude a realizar un seguimiento del propietario y el nivel de la pila de cada instancia.

El siguiente diagrama ilustra el funcionamiento del etiquetado. En este ejemplo, se han asignado dos etiquetas a cada una de las instancias — una etiqueta con la clave `Owner` y la otra con la clave `Stack`. Cada etiqueta dispone además de un valor asociado.



Le recomendamos que idee un conjunto de claves de etiqueta que cumpla sus necesidades para cada tipo de recurso. Mediante el uso de un conjunto coherente de claves de etiquetas, podrá administrar los recursos de más fácilmente. Puede buscar y filtrar los recursos en función de las etiquetas que agregue. Para obtener más información sobre cómo implementar una estrategia eficaz de etiquetado de recursos, consulte el documento técnico de AWS Tagging Best Practices (Prácticas recomendadas de etiquetado).

Las etiquetas no tienen ningún significado semántico para Amazon EC2, por lo que se interpretan estrictamente como cadenas de caracteres. Además, las etiquetas no se asignan a los recursos automáticamente. Puede editar las claves y los valores de las etiquetas y también puede eliminar etiquetas de un recurso en cualquier momento. Puede establecer el valor de una etiqueta como una cadena vacía, pero no puede asignarle un valor nulo. Si añade una etiqueta con la misma clave que una etiqueta existente en ese recurso, el nuevo valor sobrescribirá al antiguo. Si elimina un recurso, también se eliminará cualquier etiqueta asignada a dicho recurso.

> **Note**
>
> Después de eliminar un recurso, es posible que sus etiquetas permanezcan visibles en la consola, la API y la salida de la CLI durante un corto periodo de tiempo. Estas etiquetas se desasociarán del recurso de forma gradual y se eliminarán permanentemente.

Etiquetar los recursos

Puede etiquetar la mayoría de los recursos de Amazon EC2 que ya existen en la cuenta. La siguiente tabla enumera los recursos que admiten etiquetas.

Si utiliza la consola de Amazon EC2, puede aplicar etiquetas a los recursos mediante la pestaña Etiquetas de la pantalla correspondiente al recurso, o puede usar el Editor de etiquetas en la consola de AWS Resource Groups. Algunas pantallas de recursos le permiten especificar etiquetas para un recurso al crear dicho recurso; por ejemplo, una etiqueta con una clave de `Name` y un valor que especifique. En la mayoría de los casos, la consola aplica las etiquetas inmediatamente después de crear el recurso (y no durante la creación del mismo). La consola puede organizar los recursos según la etiqueta `Name`, si bien dicha etiqueta no tiene ningún significado semántico para el servicio Amazon EC2.

Si utiliza la API de Amazon EC2, la AWS CLI o un AWS SDK, puede usar la acción `CreateTags` de la API de EC2 para aplicar etiquetas a los recursos existentes. Además, algunas acciones de creación de recursos le permiten especificar etiquetas para un recurso al crear dicho recurso. Si no se pueden aplicar etiquetas durante la creación del recurso, el proceso de creación del recurso se revierte. Esto garantiza que los recursos se creen con etiquetas o, de lo contrario, no se creen y que ningún recurso se quede jamás sin etiquetar. Al etiquetar los recursos en el momento de su creación, se eliminar la necesidad de ejecutar scripts de etiquetado personalizados tras la creación del recurso. Para obtener más información acerca de cómo habilitar a los usuarios para etiquetar recursos al crear, consulte Conceder permisos para etiquetar recursos durante la creación.

En la tabla siguiente se describen los recursos de Amazon EC2 que se pueden etiquetar y aquellos que se pueden etiquetar en el momento de su creación con la API de Amazon EC2, la AWS CLI o un AWS SDK.

Compatibilidad con el etiquetado de recursos de Amazon EC2

Recurso	Admite etiquetas	Admite el etiquetado durante la creación
AFI	Sí	Sí
AMI	Sí	Sí
Tarea en paquete	No	No
Capacity Reservation	Sí	Sí

Recurso	Admite etiquetas	Admite el etiquetado durante la creación
Gateway de operador	Sí	Sí
Punto de enlace de Client VPN	Sí	Sí
Ruta de Client VPN	No	No
Gateway de cliente	Sí	Sí
Dedicated Host	Sí	Sí
Reserva de host dedicado	Sí	Sí
Opciones de DHCP	Sí	Sí
Instantánea de EBS	Sí	Sí
Volumen de EBS	Sí	Sí
EC2 Fleet	Sí	Sí
Gateway de Internet de solo salida	Sí	Sí
Dirección IP elástica	Sí	Sí
Acelerador de Elastic Graphics	Sí	No
Instancia	Sí	Sí
Ventana de evento de instancia	Sí	Sí
Volumen de almacén de instancias	N/A	N/A
Gateway de Internet	Sí	Sí

Recurso	Admite etiquetas	Admite el etiquetado durante la creación
Grupo de direcciones IP (BYOIP)	Sí	Sí
Par de claves	Sí	Sí
Plantilla de lanzamiento	Sí	Sí
Lanzar la versión de plantilla	No	No
Gateway local	Sí	No
Tabla de enrutamiento de gateway local	Sí	No
Interfaz virtual de gateway local	Sí	No
Grupo de interfaz virtual de gateway local	Sí	No
Asociación de VPC de tabla de enrutamiento de gateway local	Sí	Sí
Asociación de grupo de interfaz virtual de tabla de enrutamiento de gateway local	Sí	No
gateway NAT	Sí	Sí
ACL de red	Sí	Sí
Interfaz de red	Sí	Sí
Grupo de ubicación	Sí	Sí
Listas de prefijos	Sí	Sí

Recurso	Admite etiquetas	Admite el etiquetado durante la creación
Reserved Instance	Sí	No
Listado de Instancia reservada	No	No
Tabla de ruteo	Sí	Sí
Solicitud de flota de spot	Sí	Sí
Solicitud de instancia de spot	Sí	Sí
Grupo de seguridad	Sí	Sí
Regla del grupo de seguridad	Sí	No
Subred	Sí	Sí
Filtro de reflejo de tráfico	Sí	Sí
Sesión de reflejo de tráfico	Sí	Sí
Destino de reflejo de tráfico	Sí	Sí
Transit gateway	Sí	Sí
Dominio de multidifusión de gateway de tránsito	Sí	Sí
Tabla de ruteo de la gateway de tránsito	Sí	Sí
Vinculación VPC de la gateway de tránsito	Sí	Sí
Gateway privada virtual	Sí	Sí
VPC	Sí	Sí
Punto de conexión VPC	Sí	Sí

Recurso	Admite etiquetas	Admite el etiquetado durante la creación
Servicio de punto de enlace de la VPC	Sí	Sí
Configuración de servicio de punto de conexión de VPC	Sí	Sí
Registro de flujo de VPC	Sí	Sí
Interconexión de VPC	Sí	Sí
conexión de VPN	Sí	Sí

Puede etiquetar las instancias, volúmenes, elastic graphics, interfaces de red y solicitudes de instancias de spot al crearlos mediante el asistente de lanzamiento de instancias de Amazon EC2 en la consola de Amazon EC2. Puede etiquetar los volúmenes de EBS durante la creación en la pantalla Volúmenes o las instantáneas de EBS en la pantalla Instantáneas. Si lo prefiere, puede usar una API de Amazon EC2 de creación de recursos (por ejemplo, RunInstances) para aplicar etiquetas al crear un recurso.

En sus políticas de IAM, puede aplicar permisos de nivel de recursos basados en etiquetas a las acciones de la API de Amazon EC2 que admitan el etiquetado durante la creación para implementar un control detallado de los usuarios y los grupos que pueden etiquetar recursos durante su creación. Sus recursos están debidamente protegidos frente a la creación — las etiquetas se aplican inmediatamente a los recursos, por lo que cualquier permiso de nivel de recursos basado en etiquetas que controle el uso de los recursos es efectivo inmediatamente. Se puede realizar un seguimiento y un registro más precisos de los recursos. Puede establecer el etiquetado obligatorio de los nuevos recursos y controlar qué claves y valores de etiquetas se usan en ellos.

También puede aplicar permisos de nivel de recursos para las acciones `CreateTags` y `DeleteTags` de la API de Amazon EC2 en las políticas de IAM para controlar qué claves y valores de etiquetas se usan en los recursos existentes. Para obtener más información, consulte Ejemplo: Etiquetar recursos.

Para obtener más información acerca del etiquetado de recursos para facturación, consulte Uso de etiquetas de asignación de costos en la Guía del usuario de AWS Billing.

Restricciones de las etiquetas

Se aplican las siguientes restricciones básicas a las etiquetas:

- Número máximo de etiquetas por recurso: 50
- Para cada recurso, cada clave de etiqueta debe ser única y solo puede tener un valor.
- Longitud máxima de la clave: 128 caracteres Unicode en UTF-8
- Longitud máxima del valor: 256 caracteres Unicode en UTF-8
- Caracteres permitidos
  - Si bien EC2 admite el uso de cualquier carácter en sus etiquetas, otros servicios de AWS son más restrictivos. Los caracteres permitidos en los servicios de AWS son: letras (`a-z`, `A-Z`), números (`0-9`) y espacios representables en UTF-8, además de los siguientes caracteres: `+ - = . _ : / @`.
  - Si habilita las etiquetas de instancia en los metadatos de la instancia, la etiqueta de instancia claves solo puede utilizar letras (`a-z`, `A-Z`), números (`0-9`) y los siguientes caracteres: `+ - = . , _ : @`. Las claves de etiquetas de instancias no pueden contener espacios ni `/`, y no pueden constar solo de `.` (un punto), de `..` (dos puntos) o de `_index`. Para obtener más información, consulte Trabajar con etiquetas de instancia en los metadatos de instancia.
- Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas.
- El prefijo `aws:` se reserva para uso de AWS. Si la etiqueta tiene una clave de etiqueta con este prefijo, no puede editar ni eliminar la clave o el valor de la etiqueta. Las etiquetas que tengan el prefijo `aws:` no cuentan para el límite de etiquetas por recurso.

No puede terminar, detener ni eliminar un recurso basado únicamente en sus etiquetas; debe especificar el identificador del recurso. Por ejemplo, para eliminar instantáneas que etiquetó con una clave de etiqueta llamada `DeleteMe`, debe utilizar la acción `DeleteSnapshots` con los identificadores del recurso de las instantáneas, como `snap-1234567890abcdef0`.

Cuando etiqueta recursos públicos o compartidos, las etiquetas que asigne solo están disponibles para su cuenta de AWS; ninguna otra cuenta de AWS tendrá acceso a esas etiquetas. Para el control de acceso a recursos compartidos basado en etiquetas, cada cuenta de AWS debe asignar su propio conjunto de etiquetas para controlar el acceso al recurso.

No puede etiquetar todos los recursos. Para obtener más información, consulte Compatibilidad con el etiquetado de recursos de Amazon EC2.

Administración de etiquetas y accesos

Si utiliza AWS Identity and Access Management (IAM), puede controlar qué usuarios de su cuenta de AWS tienen permiso para crear, editar o eliminar etiquetas. Para obtener más información, consulte Conceder permisos para etiquetar recursos durante la creación.

También puede usar etiquetas de recursos para implementar el control basado en atributos (ABAC). Puede crear directivas de IAM que permitan operaciones basadas en las etiquetas del recurso. Para obtener más información, consulte Control del acceso a recursos de EC2 mediante etiquetas de recursos.

Etiquetar los recursos para facturación

Puede usar etiquetas para organizar la factura de AWS de modo que refleje su propia estructura de costos. Para ello, inscríbase para obtener una factura de la cuenta de AWS que incluya valores de clave de etiquetas. Para obtener más información sobre la configuración de un informe de asignación de costos con etiquetas, consulte Informe de asignación de costos mensual en la Guía del usuario de AWS Billing. Para ver el costo de los recursos combinados, puede organizar la información de facturación basada en los recursos que tienen los mismos valores de clave de etiqueta. Por ejemplo, puede etiquetar varios recursos con un nombre de aplicación específico y luego organizar su información de facturación para ver el costo total de la aplicación en distintos servicios. Para obtener más información, consulte Uso de etiquetas de asignación de costos en la Guía del usuario de AWS Billing.

> **Note**
>
> Si acaba de habilitar la realización de informes, los datos correspondientes al mes actual estarán disponibles para su visualización transcurridas 24 horas.

Las etiquetas de asignación de costos pueden indicar qué recursos influyen en los costos. Sin embargo, eliminar o desactivar los recursos no reduce necesariamente los costos. Por ejemplo, los datos de una instantánea a los que se haga referencia en otra instantánea se conservan incluso si se elimina la instantánea que contiene los datos originales. Para obtener más información, consulte Volúmenes e instantáneas de Amazon Elastic Block Store en la Guía del usuario de AWS Billing.

> **Note**
>
> Las direcciones IP elásticas que se han etiquetado no aparecen en el informe de asignación de costos.

Trabajar con etiquetas mediante la consola

Puede utilizar la consola de Amazon EC2 para mostrar las etiquetas de un recurso individual y para aplicar o eliminar etiquetas en uno o varios recursos a la vez.

Puede utilizar el Editor de etiquetas de la consola de AWS Resource Groups para mostrar las etiquetas de todos sus recursos de Amazon EC2 en todas las regiones. Puede ver etiquetas por recurso y por tipo de recurso, así como los tipos de recursos asociados a una etiqueta determinada. Puede aplicar o eliminar etiquetas en varios recursos y varios tipos de recursos a la vez. Editor de etiquetas proporciona una forma unificada y centralizada de crear y administrar sus etiquetas. Para obtener más información, consulte Guía del usuario para el etiquetado de recursos de AWS.

Tareas

- Mostrar etiquetas
- Agregar y eliminar etiquetas en un recurso individual
- Agregar y eliminar etiquetas para varios recursos
- Agregar una etiqueta cuando lanza una instancia
- Filtrar una lista de recursos por etiqueta

Mostrar etiquetas

Puede mostrar las etiquetas de un recurso individual en la consola de Amazon EC2. Para mostrar las etiquetas de todos sus recursos, utilice el Editor de etiquetas de la consola de AWS Resource Groups.

Mostrar etiquetas de un recurso individual

Al seleccionar una página específica de un recurso en la consola de Amazon EC2, se muestra una lista de dicho recurso. Por ejemplo, si selecciona Instances (Instancia[s]) en el panel de navegación, la consola muestra una lista de las instancias Amazon EC2. Al seleccionar un recurso de una de estas listas (por ejemplo, una instancia), si el recurso admite etiquetas, puede ver y administrar sus

etiquetas. En la mayoría de las páginas de recursos, puede ver las etiquetas al elegir la pestaña Tags (Etiquetas).

Puede agregar una columna a la lista de recursos para mostrar todos los valores para las etiquetas con la misma clave. Esta columna permite ordenar y filtrar la lista de recursos por etiqueta.

New console

Para agregar una columna a la lista de recursos para mostrar las etiquetas

1. En la consola de EC2, elija el icono Preferencias (el engranaje) de la esquina superior derecha de la pantalla.
2. En el cuadro de diálogo Preferencias, en Columnas de etiqueta (abajo a la izquierda), seleccione una de las claves de etiqueta más y, a continuación, elija Confirmar.

Old console

Existen dos maneras de agregar una nueva columna a la lista de recursos para mostrar las etiquetas.

- En la pestaña Tags (Etiquetas), seleccione Show Column (Mostrar columna). Se añade una nueva columna en la consola.
- Elija el icono con forma de engranaje Show/Hide Columns (Mostrar/ocultar columnas) y, en cuadro de diálogo Show/Hide Columns (Mostrar/ocultar columnas), seleccione la clave de etiqueta en Your Tag Keys (Sus claves de etiquetas).

Mostrar etiquetas para múltiples recursos

Puede mostrar etiquetas en varios recursos mediante el Editor de etiquetas de la consola de AWS Resource Groups. Para obtener más información, consulte Guía del usuario para el etiquetado de recursos de AWS.

Agregar y eliminar etiquetas en un recurso individual

Puede administrar las etiquetas para un recurso individual directamente desde la página del recurso.

Para añadir una etiqueta a un recurso individual

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

2. En la barra de navegación, seleccione la región donde se encuentra el recurso que desea etiquetar. Para obtener más información, consulte Ubicaciones de los recursos.
3. En el panel de navegación, seleccione un tipo de recurso (por ejemplo, Instances (Instancia[s])).
4. Seleccione el recurso de la lista de recursos y elija Tags (Etiquetas).
5. Elija la pestaña Administrar etiquetas y, a continuación, elija Agregar nueva etiqueta. Escriba la clave y el valor de para la etiqueta. Elija Agregar nueva etiqueta para cada etiqueta adicional. Cuando haya terminado de agregar etiquetas, elija Save (Guardar).

Para eliminar una etiqueta de un recurso individual

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la barra de navegación, seleccione la región donde se encuentra el recurso al cual desea eliminar la etiqueta. Para obtener más información, consulte Ubicaciones de los recursos.
3. En el panel de navegación, elija un tipo de recurso (por ejemplo, Instances (Instancia[s])).
4. Seleccione el recurso de la lista de recursos y elija Tags (Etiquetas).
5. Elija Manage tags (Administrar etiquetas). Por cada etiqueta a eliminar, elija Quitar. Cuando termine de quitar las etiquetas, elija Save (Guardar).

Agregar y eliminar etiquetas para varios recursos

Para agregar una etiqueta a varios recursos

1. Abra el Editor de etiquetas en la consola de AWS Resource Groups en https://console.aws.amazon.com/resource-groups/tag-editor.
2. En Regiones, seleccione una o varias regiones donde se encuentran los recursos a los cuales desea etiquetar.
3. En Tipos de recursos, seleccione el tipo de recursos que desee etiquetar (por ejemplo, AWS::EC2::Instance).
4. Seleccione Buscar recursos.
5. En Resultados de la búsqueda de recursos, seleccione la casilla de verificación situada junto a cada recurso que desee etiquetar.
6. Seleccione Administrar las etiquetas de los recursos seleccionados.

7. En Editar etiquetas de todos los recursos seleccionados, elija Agregar etiqueta y, a continuación, introduzca la nueva clave y el valor de la etiqueta. Elija Add tag (Agregar etiqueta) para cada etiqueta adicional.

> **Note**
>
> Si añade una nueva etiqueta con la misma clave que una etiqueta existente, la nueva etiqueta sobrescribirá a la antigua.

8. Seleccione Revisar y aplicar cambios en la etiqueta.
9. Elija Apply changes to all selected (Aplicar cambios a todo lo seleccionado).

Para eliminar una etiqueta de múltiples recursos

1. Abra el Editor de etiquetas en la consola de AWS Resource Groups en https://console.aws.amazon.com/resource-groups/tag-editor.
2. En Regiones, seleccione las regiones donde se encuentran los recursos a los cuales desea desetiquetar.
3. En Tipos de recursos, seleccione el tipo de recursos que desee desetiquetar (por ejemplo, AWS::EC2::Instance).
4. Seleccione Buscar recursos.
5. En Resultados de la búsqueda de recursos, seleccione la casilla de verificación situada junto a cada recurso que desee desetiquetar.
6. Seleccione Administrar las etiquetas de los recursos seleccionados.
7. En Editar etiquetas de todos los recursos seleccionados, seleccione Eliminar etiqueta junto a la etiqueta que desee eliminar.
8. Seleccione Revisar y aplicar cambios en la etiqueta.
9. Elija Apply changes to all selected (Aplicar cambios a todo lo seleccionado).

Agregar una etiqueta cuando lanza una instancia

New console

Para agregar una etiqueta mediante el asistente de instancias de lanzamiento

1. Desde la barra de navegación, seleccione la región para la instancia. Esta elección es importante porque algunos recursos de Amazon EC2 pueden compartirse entre varias regiones, mientras que otros no. Seleccione la región que mejor se adapte a sus necesidades. Para obtener más información, consulte Ubicaciones de los recursos.
2. Seleccione iniciar instancia.
3. En Name and tags (Nombre y etiquetas), puede indicar un nombre descriptivo para la instancia y especificar etiquetas.

   El nombre de la instancia es una etiqueta, donde la clave es Name (Nombre) y el valor es el nombre que especifique. Puede etiquetar la instancia, los volúmenes, elastic graphics y las interfaces de red. Para las instancias de spot, solo puede etiquetar la solicitud de instancia de spot.

   Especificar un nombre de instancia y etiquetas adicionales es opcional.

   - En Name (Nombre), ingrese un nombre descriptivo para la instancia. Si no especifica un nombre, la instancia se puede identificar mediante su ID, que se genera automáticamente al iniciar la instancia.
   - Para agregar otras etiquetas, elija Add additional tag (Agregar etiqueta adicional). Elija Add tag (Agregar etiqueta) y, a continuación, ingrese una clave y un valor, y seleccione el tipo de recurso que desea etiquetar. Elija Add tag (Agregar etiqueta) para cada etiqueta adicional.
4. En Application and OS Images (Amazon Machine Image) (Imágenes de aplicaciones y sistema operativo [Imagen de máquina de Amazon]), elija el sistema operativo (SO) para la instancia y, a continuación, una AMI. Para obtener más información, consulte Imágenes de aplicaciones y sistema operativo (Imagen de máquina de Amazon).
5. (Opcional) En Par de claves (inicio), para Nombre de par de claves seleccione un par de claves existente o cree uno nuevo.
6. Mantenga todos los demás campos en sus valores predeterminados o elija valores específicos para la configuración de instancia que desee. Para obtener más información acerca de los campos, consulte iniciar una instancia mediante parámetros definidos.

7. En el panel Summary (Resumen), revise la configuración y, a continuación, elija Launch instance (Lanzar instancia).

Old console

Para agregar una etiqueta mediante el asistente de instancias de lanzamiento

1. Desde la barra de navegación, seleccione la región para la instancia. Esta elección es importante porque algunos recursos de Amazon EC2 pueden compartirse entre varias regiones, mientras que otros no. Seleccione la región que mejor se adapte a sus necesidades. Para obtener más información, consulte Ubicaciones de los recursos.
2. Elija Launch Instance.
3. En la página Choose an Amazon Machine Image (AMI) (Elegir una Amazon Machine Image (AMI)), se muestra una lista de configuraciones básicas denominadas Amazon Machine Images (AMI). Seleccione la AMI que vaya a utilizar y elija Select (Seleccionar). Para obtener más información, consulte Buscar una AMI.
4. En la página Configure Instance Details (Configurar detalles de instancia), ajuste la configuración de la instancia según sea necesario y, a continuación, elija Next: Add Storage (Siguiente: Agregar almacenamiento).
5. En la página Add Storage (Agregar almacenamiento), puede especificar volúmenes de almacenamiento adicionales para la instancia. Cuando haya terminado, elija Next: Add Tags (Siguiente: Añadir etiquetas).
6. En la página Add Tags (Añadir etiquetas), especifique las etiquetas para la instancia, los volúmenes o ambos. Elija Add another tag (Añadir otra etiqueta) para añadir más de una etiqueta a la instancia. Elija Next: Configure Security Group (Siguiente: Configurar grupo de seguridad) cuando haya terminado.
7. En la página Configure Security Group (Configurar grupo de seguridad), puede elegir uno de los grupos de seguridad existentes que tiene o bien permitir que el asistente cree uno nuevo. Cuando haya terminado, elija Review and Launch (Revisar y lanzar).
8. Revise la configuración. Cuando esté satisfecho con las opciones seleccionadas, elija Launch (Lanzar). Seleccione un par de claves existente o cree uno nuevo, active la casilla de verificación de confirmación y, a continuación, elija Launch Instances (Lanzar instancias).

Filtrar una lista de recursos por etiqueta

Puede filtrar la lista de recursos en función de una o varias claves y valores de etiquetas.

Para filtrar una lista de recursos por etiqueta en la consola de Amazon EC2

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione un tipo de recurso (por ejemplo, Instances (Instancia[s])).
3. Elija el campo de búsqueda.
4. En la lista, en Etiquetas, elija la clave de etiqueta.
5. Elija el valor de etiqueta correspondiente de la lista.
6. Cuando haya terminado, quite el filtro.

Para obtener más información sobre el uso de filtros en la consola de Amazon EC2, consulte Enumerar y filtrar los recursos.

Para filtrar varios recursos en varias regiones por etiqueta mediante el Editor de etiquetas

Puede utilizar el Editor de etiquetas de la consola de AWS Resource Groups para filtrar varios recursos de varias regiones por etiqueta. Para obtener más información, consulte Buscar recursos para etiquetar en la Guía del usuario para el etiquetado de recursos de AWS.

Trabajar con etiquetas mediante la línea de comandos

Puede agregar etiquetas a muchos recursos de EC2 al crearlos, mediante el parámetro de especificaciones de etiquetas para el comando create. Puede ver las etiquetas de un recurso mediante el comando describe del recurso. También puede agregar, actualizar o eliminar etiquetas de los recursos existentes mediante los siguientes comandos.

Tarea	AWS CLI	AWS Tools for Windows PowerShell
Agregar o sobrescribir una o varias etiquetas.	create-tags	New-EC2Tag
Eliminar una o varias etiquetas.	delete-tags	Remove-EC2Tag

Tarea	AWS CLI	AWS Tools for Windows PowerShell
Describir una o varias etiquetas.	describe-tags	Get-EC2Tag

Tareas

- Agregar etiquetas en la creación de recursos
- Agregar etiquetas a un recurso existente
- Describir recursos etiquetados

Agregar etiquetas en la creación de recursos

El siguiente ejemplo demuestra cómo aplicar etiquetas al crear recursos.

> **Note**
>
> El modo en que introduzca parámetros con formato JSON en la línea de comandos varía en función de su sistema operativo.
>
> - Linux, macOS, o Unix y Windows PowerShell: utilice comillas simples (') para entrecomillar la estructura de datos JSON.
> - Windows: omita las comillas simples cuando utilice los comandos en la línea de comandos de Windows.
>
> Para obtener más información, consulte Especificación de valores de parámetros para la AWS CLI.

Example Ejemplo: lanzar una instancia y aplicar etiquetas a la instancia y al volumen

El siguiente comando run-instances lanza una instancia y aplica una etiqueta con la clave **`webserver`** y el valor **`production`** a la instancia. El comando también aplica una etiqueta con la clave **`cost-center`** y el valor **`cc123`** a cualquier volumen de EBS que se cree (en este caso, el volumen raíz).

```
aws ec2 run-instances \
```

```
    --image-id ami-abc12345 \
    --count 1 \
    --instance-type t2.micro \
    --key-name MyKeyPair \
    --subnet-id subnet-6e7f829e \
    --tag-specifications
 'ResourceType=instance,Tags=[{Key=webserver,Value=production}]'
 'ResourceType=volume,Tags=[{Key=cost-center,Value=cc123}]'
```

Puede aplicar las mismas claves y valores de etiqueta tanto a las instancias como a los volúmenes durante el lanzamiento. El siguiente comando lanza una instancia y aplica una etiqueta con una clave de **`cost-center`** y un valor de **`cc123`** tanto a la instancia como a cualquier volumen de EBS que se cree.

```
aws ec2 run-instances \
    --image-id ami-abc12345 \
    --count 1 \
    --instance-type t2.micro \
    --key-name MyKeyPair \
    --subnet-id subnet-6e7f829e \
    --tag-specifications 'ResourceType=instance,Tags=[{Key=cost-center,Value=cc123}]'
 'ResourceType=volume,Tags=[{Key=cost-center,Value=cc123}]'
```

Example Ejemplo: crear un volumen y aplicar una etiqueta

El siguiente comando create-volume crea un volumen y aplica dos etiquetas: **`purpose=production`** y **`cost-center=cc123`**.

```
aws ec2 create-volume \
    --availability-zone us-east-1a \
    --volume-type gp2 \
    --size 80 \
    --tag-specifications 'ResourceType=volume,Tags=[{Key=purpose,Value=production},
{Key=cost-center,Value=cc123}]'
```

Agregar etiquetas a un recurso existente

En los ejemplos siguientes se muestra cómo agregar etiquetas a un recurso existente mediante el comando create-tags.

Example Ejemplo: agregar una etiqueta a un recurso

El comando siguiente agrega la etiqueta **Stack=production** a la imagen especificada o sobrescribe una etiqueta existente para la AMI en la que la clave de etiqueta es **Stack**. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

```
aws ec2 create-tags \
    --resources ami-78a54011 \
    --tags Key=Stack,Value=production
```

Example Ejemplo: agregar etiquetas a varios recursos

Este ejemplo añade (o sobrescribe) dos etiquetas para una AMI y una instancia. Una de las etiquetas contiene solo una clave (**webserver**), sin valor (establecemos el valor en una cadena vacía). La otra etiqueta consta de una clave (**stack**) y un valor (**Production**). Si el comando se ejecuta correctamente, no se muestra ningún resultado.

```
aws ec2 create-tags \
    --resources ami-1a2b3c4d i-1234567890abcdef0 \
    --tags Key=webserver,Value=  Key=stack,Value=Production
```

Example Ejemplo: agregar etiquetas con caracteres especiales

Este ejemplo agrega la etiqueta **[Group]=test** a una instancia. Los corchetes (**[** y **]**) son caracteres especiales, que deben ser incluirse en el carácter de escape.

Si utiliza Linux u OS X, para incluir en el carácter de escape los caracteres especiales, encierre el elemento con carácter especial entre comillas dobles (**"**) y después incluya la estructura completa de clave y valor entre comillas simples (**'**).

```
aws ec2 create-tags \
    --resources i-1234567890abcdef0 \
    --tags 'Key="[Group]",Value=test'
```

Si está utilizando Windows, para incluir en el carácter de escape los caracteres especiales, encierre el elemento que tiene caracteres especiales con comillas dobles (") y, a continuación, preceda cada carácter de comillas dobles con una barra invertida (****) de la siguiente manera:

```
aws ec2 create-tags ^
    --resources i-1234567890abcdef0 ^
```

```
    --tags Key=\"[Group]\",Value=test
```

Si está utilizando Windows PowerShell, para incluir en el carácter de escape los caracteres especiales, encierre el valor que tiene caracteres especiales con comillas dobles (**"**), preceda cada carácter de comillas dobles de una barra invertida (****) y, a continuación, encierre toda la estructura de clave y valor con comillas simples (**'**) de la siguiente manera:

```
aws ec2 create-tags `
    --resources i-1234567890abcdef0 `
    --tags 'Key=\"[Group]\",Value=test'
```

Describir recursos etiquetados

En los ejemplos siguientes se muestra cómo utilizar filtros con describe-instances para ver instancias con etiquetas específicas. Todos los comandos describe de EC2 utilizan esta sintaxis para filtrar por etiqueta en un único tipo de recurso. También puede utilizar el comando describe-tags para filtrar por etiqueta entre los tipos de recursos EC2.

Example Ejemplo: describir instancias con la clave de etiqueta especificada

En el siguiente comando se describen las instancias con una etiqueta **`Stack`**, con independencia del valor de la etiqueta.

```
aws ec2 describe-instances \
    --filters Name=tag-key,Values=Stack
```

Example Ejemplo: describir instancias con la etiqueta especificada

En el siguiente comando se describen las instancias con la etiqueta **`Stack=production`**.

```
aws ec2 describe-instances \
    --filters Name=tag:Stack,Values=production
```

Example Ejemplo: describir instancias con el valor de etiqueta especificado

En el siguiente comando se describen las instancias con una etiqueta con el valor **`production`**, con independencia de la clave de etiqueta.

```
aws ec2 describe-instances \
    --filters Name=tag-value,Values=production
```

Example Ejemplo: describa todos los recursos EC2 con la etiqueta especificada

El siguiente comando describe todos los recursos EC2 con la etiqueta **`Stack=Test`**.

```
aws ec2 describe-tags \
    --filters Name=key,Values=Stack Name=value,Values=Test
```

Trabajar con etiquetas de instancia en los metadatos de instancia

Puede acceder a las etiquetas de una instancia desde los metadatos de la instancia. Al acceder a las etiquetas desde los metadatos de la instancia, ya no tendrá que utilizar las llamadas a la API `DescribeInstances` o `DescribeTags` para recuperar información de etiquetas, lo que reduce las transacciones de la API por segundo y permite que las recuperaciones de etiquetas se escalen según el número de instancias que controla. Además, los procesos locales que se ejecutan en una instancia pueden ver la información de etiqueta de la instancia directamente desde los metadatos de la instancia.

De forma predeterminada, las etiquetas no están disponibles en los metadatos de la instancia; debe permitir explícitamente el acceso. Puede permitir el acceso durante el lanzamiento de la instancia o después del lanzamiento en una instancia en ejecución o detenida. También puede permitir el acceso a las etiquetas especificándolo en una plantilla de lanzamiento. Las instancias que se lanzan mediante la plantilla permiten el acceso a las etiquetas de los metadatos de la instancia.

Si agrega o elimina una etiqueta de instancia, los metadatos de la instancia se actualizan mientras se ejecuta la instancia, sin necesidad de detener e iniciar la instancia.

Temas

- Permitir acceso a etiquetas en metadatos de instancia
- Desactivar el acceso a las etiquetas en metadatos de instancia
- Ver si se permite el acceso a las etiquetas en los metadatos de instancia
- Recuperar etiquetas desde los metadatos de instancia

Permitir acceso a etiquetas en metadatos de instancia

De forma predeterminada, no hay acceso a las etiquetas de instancia en los metadatos de la instancia. Para cada instancia, debe permitir el acceso explícitamente mediante uno de los métodos siguientes.

Para permitir acceso a etiquetas en metadatos de instancia mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Seleccione una instancia y, a continuación, elija Actions (Acciones), Instance settings (Configuración de la instancia), Allow tags in instance metadata (Permitir etiquetas en metadatos de instancia).
4. Para permitir el acceso a las etiquetas de los metadatos de instancia, seleccione la casilla Allow (Permitir).
5. Seleccione Guardar.

Para permitir acceso a etiquetas en metadatos de instancia durante el lanzamiento mediante la AWS CLI

Utilice el comando run-instances y establezca `InstanceMetadataTags` en `enabled`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c3.large \
    ...
    --metadata-options "InstanceMetadataTags=enabled"
```

Para permitir el acceso a etiquetas de metadatos de instancia en una instancia en ejecución o detenida mediante la AWS CLI

Utilice el comando modify-instance-metadata-options y establezca `--instance-metadata-tags` en `enabled`.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-123456789example \
    --instance-metadata-tags enabled
```

Desactivar el acceso a las etiquetas en metadatos de instancia

Para desactivar el acceso a las etiquetas de instancia en los metadatos de instancia, utilice uno de los métodos siguientes. No es necesario desactivar el acceso a las etiquetas de instancia en los metadatos de instancia durante el lanzamiento porque está desactivado de forma predeterminada.

Para desactivar el acceso a etiquetas en metadatos de instancia mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Seleccione una instancia y, a continuación, elija Actions (Acciones), Instance settings (Configuración de la instancia), Allow tags in instance metadata (Permitir etiquetas en metadatos de instancia).
4. Para desactivar el acceso a las etiquetas de los metadatos de instancia, desactive la casilla Allow (Permitir).
5. Seleccione Guardar.

Para desactivar el acceso a etiquetas en metadatos de instancia mediante la AWS CLI

Utilice el comando modify-instance-metadata-options y establezca `--instance-metadata-tags` en `disabled`.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-123456789example \
    --instance-metadata-tags disabled
```

Ver si se permite el acceso a las etiquetas en los metadatos de instancia

En cada instancia, puede utilizar la consola de Amazon EC2 o la AWS CLI para ver si se permite el acceso a las etiquetas de instancia de los metadatos de instancia.

Para ver si está permitido el acceso a etiquetas en metadatos de instancia mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instancias y, a continuación, seleccione una instancia.
3. En la pestaña Details (Detalles), marque el campo Allow tags in instance metadata (Permitir etiquetas en los metadatos de la instancia). Si el valor es Enabled (Habilitadas), se permiten etiquetas en los metadatos de instancia. Si el valor es Disabled (Deshabilitadas), no se permitirán las etiquetas en los metadatos de instancia.

Para ver si se permite el acceso a las etiquetas en los metadatos de instancia mediante la AWS CLI

Use el comando describe-instances y especifique el ID de la instancia.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0
```

La siguiente salida de ejemplo está truncada por falta de espacio. El parámetro `"InstanceMetadataTags"` indica si se permiten las etiquetas en los metadatos de la instancia. Si el valor es `enabled`, se permiten etiquetas en los metadatos de instancia. Si el valor es `disabled`, no se permitirá el uso de etiquetas en los metadatos de instancia.

```
{
    "Reservations": [
        {
            "Groups": [],
            "Instances": [
                {
                    "AmiLaunchIndex": 0,
                    "ImageId": "ami-0abcdef1234567890",
                    "InstanceId": "i-1234567890abcdef0",
   ...

   "MetadataOptions": {
   "State": "applied",
   "HttpTokens": "optional",
   "HttpPutResponseHopLimit": 1,
   "HttpEndpoint": "enabled",
   "HttpProtocolIpv6": "disabled",
   "InstanceMetadataTags": "enabled"
   },
   ...
```

Recuperar etiquetas desde los metadatos de instancia

Si se permiten etiquetas de instancia en los metadatos de la instancia, se puede acceder a la categoría `tags/instance` desde los metadatos de la instancia. Para obtener ejemplos sobre cómo recuperar etiquetas de los metadatos de la instancia, consulte Obtener las etiquetas de instancia de una instancia.

Agregar etiquetas a un recurso mediante CloudFormation

Con los tipos de recursos de Amazon EC2, especifica etiquetas mediante una propiedad `Tags` o `TagSpecifications`.

En los siguientes ejemplos se agrega la etiqueta **`Stack=Production`** a AWS::EC2::Instance mediante su propiedad `Tags`.

Example Ejemplo: Tags en YAML

```
Tags:
  - Key: "Stack"
    Value: "Production"
```

Example Ejemplo: Tags en JSON

```
"Tags": [
    {
        "Key": "Stack",
        "Value": "Production"
    }
]
```

En los ejemplos siguientes se agrega la etiqueta **`Stack=Production`** a AWS::EC2::LaunchTemplate LaunchTemplateData mediante su propiedad `TagSpecifications`.

Example Ejemplo: TagSpecifications en YAML

```
TagSpecifications:
  - ResourceType: "instance"
    Tags:
    - Key: "Stack"
      Value: "Production"
```

Example Ejemplo: TagSpecifications en JSON

```
"TagSpecifications": [
    {
        "ResourceType": "instance",
        "Tags": [
            {
                "Key": "Stack",
                "Value": "Production"
            }
        ]
    }
```

```
]
```

Cuotas de servicio de Amazon EC2

Amazon EC2 proporciona distintos recursos que puede utilizar. Estos recursos incluyen imágenes, instancias, volúmenes e instantáneas. Cuando cree su Cuenta de AWS, estableceremos las cuotas (también denominadas “límites”) predeterminadas de estos recursos por regiones. Por ejemplo, hay un número máximo de instancias que puede lanzar en una región. Si lanzara una instancia en la región EE.UU. Oeste (Oregón), por ejemplo, la solicitud no puede hacer que el uso supere el número máximo de instancias de esa región.

La consola de Service Quotas es una ubicación central donde puede ver y administrar sus cuotas de servicios de AWS y solicitar un aumento de cuota para muchos de los recursos que utiliza. Utilice la información sobre las cuotas que proporcionamos para administrar la infraestructura de AWS. Planifique la solicitud del aumento de las cuotas antes del momento en que lo necesite.

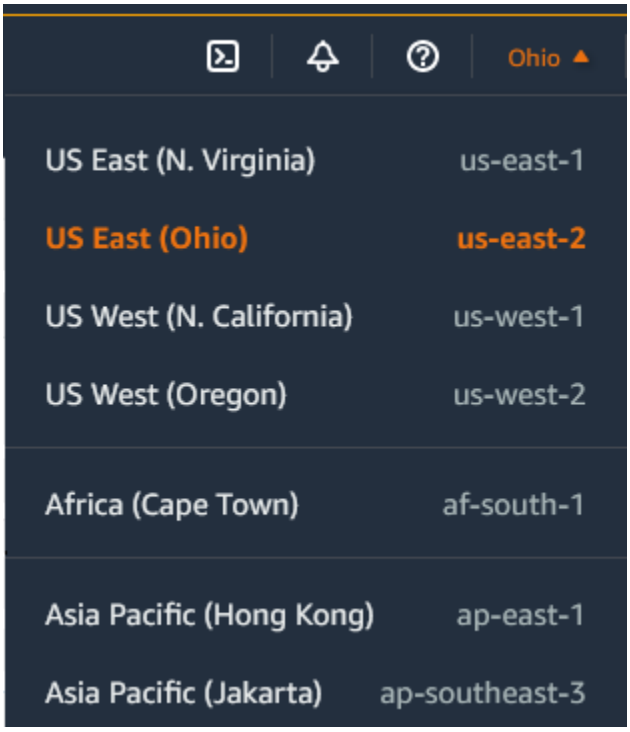
Para obtener más información, consulte Amazon EC2 endpoints and quotas y Amazon EBS endpoints and quotas en Referencia general de Amazon Web Services.

Visualización de las cuotas actuales

Puede ver las cuotas de cada región mediante la consola de Service Quotas.

Visualización de las cuotas actuales desde la consola de Service Quotas

1. Abra la consola de Service Quotas en https://console.aws.amazon.com/servicequotas/home/services/ec2/quotas/.
2. Desde la barra de navegación (parte superior de la pantalla), seleccione una región.



3. Utilice el campo de filtro para filtrar la lista por nombre de recurso. Por ejemplo, ingrese **`On-Demand`** para localizar las cuotas de las instancias bajo demanda.
4. Para ver más información, elija el nombre de la cuota para abrir la página de detalles de la cuota.

Solicitar un aumento

Puede solicitar un aumento de la cuota para cada región.

Para solicitar un aumento, visite la Consola de Service Quotas.

1. Abra la consola de Service Quotas en https://console.aws.amazon.com/servicequotas/home/services/ec2/quotas/.
2. Desde la barra de navegación (parte superior de la pantalla), seleccione una región.
3. Utilice el campo de filtro para filtrar la lista por nombre de recurso. Por ejemplo, ingrese **`On-Demand`** para localizar las cuotas de las instancias bajo demanda.
4. Si la cuota es ajustable, selecciónela y elija Solicitar aumento de cuota.
5. En Cambiar valor de cuota, ingrese el nuevo valor.
6. Seleccione Request (Solicitar).

7. Para ver las solicitudes pendientes o resueltas recientemente, elija Panel en el panel de navegación. Para las solicitudes pendientes, seleccione el estado de la solicitud para abrir la recepción de solicitud. El estado inicial de una solicitud es Pendiente. Después de que el estado cambie a Cuota solicitada, verá el número de caso con AWS Support. Elija el número de caso para abrir el ticket para su solicitud.

Para obtener más información, incluida la forma de utilizar la AWS CLI o los SDK o para solicitar un aumento de cuota, consulte Solicitud de un aumento de cuota en la Guía del usuario de Service Quotas.

Restricción en el correo electrónico enviado a través del puerto 25

En todas las instancias, Amazon EC2 restringe el tráfico saliente en las direcciones IP públicas al puerto 25 de forma predeterminada. Puede solicitar que se elimine esta restricción. Para obtener más información, consulte ¿Cómo puedo eliminar la restricción en el puerto 25 de mi instancia de Amazon EC2 o de la función de Lambda?

> **Note**
>
> Esta restricción no se aplica al tráfico saliente enviado por el puerto 25 a:
>
> - Direcciones IP en el bloque de CIDR principal de la VPC en la que existe la interfaz de red de origen.
> - Direcciones IP en los CIDR definidos en RFC 1918, RFC 6598 y RFC 4193.

Solucionar problemas de instancias de EC2

Los procedimientos y las sugerencias siguientes ayudan a solucionar los problemas que se presentan con las instancias de Amazon EC2.

Contenido

Problemas comunes con las instancias de Windows

A continuación, se ofrecen algunas sugerencias para solucionar problemas comunes con instancias EC2 para Windows Server.

Problemas

- No se puede obtener el resultado de la consola
- Windows Server 2012 R2 no está disponible en la red
- Colisión de firma de disco

Los volúmenes de EBS no se inicializan en Windows Server 2016 y 2019

Las instancias creadas a partir de imágenes de máquina de Amazon (AMI) para Windows Server 2016 y 2019 utilizan el agente EC2Launch versión 1 para una serie de tareas de inicio, entre ellas la inicialización de volúmenes de EBS. De forma predeterminada, EC2Launch versión 1 no inicia volúmenes secundarios. Sin embargo, puede configurar EC2Launch versión 1 para inicializar estos discos automáticamente, de la siguiente manera.

Asignar las letras de unidad con los volúmenes

1. Conéctese a la instancia que desea configurar y abra el archivo `C:\ProgramData\Amazon\EC2-Windows\Launch\Config\DriveLetterMappingConfig.json` en un editor de texto.
2. Especifique la configuración de volumen de la siguiente manera:

```
{
"driveLetterMapping": [
 {
   "volumeName": "sample volume",
   "driveLetter": "H"
 }]
}
```

3. Guarde los cambios y cierre el archivo.
4. Abra Windows PowerShell y utilice el siguiente comando para ejecutar el script de EC2Launch versión 1 que inicializa los discos:

```
PS C:\>  C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1
```

   Para inicializar los discos cada vez que se arranca la instancia, añada la marca `-Schedule` de la siguiente manera:

```
PS C:\>  C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1 -
Schedule
```

El agente EC2Launch versión 1 puede ejecutar scripts de inicialización de instancias como `initializeDisks.ps1` en paralelo con el script `InitializeInstance.ps1`. Si el script `InitializeInstance.ps1` reinicia la instancia, ya que puede interrumpir otras tareas programadas que se ejecutan al iniciar la instancia. Para evitar posibles conflictos, le recomendamos que agregue lógica a su script `initializeDisks.ps1` para garantizar que la inicialización de la instancia haya finalizado primero.

> **Note**
>
> Si el script de EC2Launch no lanza los volúmenes, asegúrese de que estén en línea. Si los volúmenes no están en línea, ejecute el siguiente comando para conectar todos los discos.
>
> ```
> PS C:\> Get-Disk | Where-Object IsOffline -Eq $True | Set-Disk -IsOffline
>  $False
> ```

Arranque una instancia EC2 de Windows en modo DSRM (Directory Services Restore Mode)

Si una instancia que ejecuta Microsoft Active Directory experimenta un error del sistema u otro problema crítico, puede solucionarlo arrancando la instancia en una versión especial del modo seguro denominada Directory Services Restore Mode (DSRM). En modo DSRM, puede reparar o recuperar Active Directory.

Soporte de los controladores para DSRM

El modo de habilitar DSRM y arrancar en la instancia depende de los controladores que ejecute la instancia. En la consola de EC2, puede ver los detalles de las versiones de los controladores de una instancia del registro del sistema. En la tabla siguiente se muestran los controladores admitidos para DSRM.

Versiones de controlador	¿Admite DSRM?	Pasos siguientes
Citrix PV 5.9	No	Restaure la instancia desde un backup. No puede habilitar DSRM.
AWS PV 7.2.0	No	Si bien DSRM no se admite con este controlador, puede separar el volumen raíz de la instancia, tomar una instantánea del volumen o crear una AMI, y adjuntarlo a otra instancia de la misma zona de disponibilidad como un volumen secundario. Después, puede habilitar DSRM (como se describe en esta sección).
AWS PV 7.2.2 y posterior	Sí	Separe el volumen raíz, adjúntelo a otra instancia y habilite DSRM (como se describe en esta sección).
Redes mejoradas	Sí	Separe el volumen raíz, adjúntelo a otra instancia y habilite DSRM (como se describe en esta sección).

Para obtener información acerca de cómo habilitar redes mejoradas, consulte the section called “Elastic Network Adapter (ENA)”. Para obtener información sobre la actualización de los controladores PV de AWS, consulte Actualizar los controladores PV en instancias de Windows.

Configuración de una instancia para arrancar en modo DSRM

Las instancias de Windows de EC2 no tienen conexión de red hasta que el sistema operativo está en ejecución. Por esta razón, no puede presionar la tecla F8 del teclado para seleccionar una opción de arranque. Debe seguir uno de estos procedimientos para arrancar una instancia de Windows Server de EC2 en modo DSRM.

Si sospecha que Active Directory se ha dañado y que la instancia sigue ejecutándose, puede configurar la instancia para que arranque en modo DSRM usando el cuadro de diálogo de configuración del sistema o el símbolo del sistema.

Para arrancar una instancia online en DSRM usando el cuadro de diálogo de configuración del sistema

1. En el cuadro de diálogo Ejecutar, escriba `msconfig` y pulse Intro.

2. Elija la pestaña Arranque.
3. En Opciones de arranque elija Arranque seguro.
4. Elija Reparar Active Directory y, a continuación, elija Aceptar. El sistema le solicita que reinicie el servidor.

Para reiniciar una instancia online en modo DSRM con la línea de comandos

En una ventana del símbolo del sistema, ejecute el siguiente comando:

```
bcdedit /set safeboot dsrepair
```

Si la instancia no está en línea y es inaccesible, debe separar el volumen raíz y adjuntarlo a otra instancia para habilitar el modo DSRM.

Para arrancar una instancia que no está en línea en modo DSRM

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancias).
3. Localice y seleccione la instancia afectada. Elija Instance state (Estado de la instancia) y Stop instance (Detener instancia).
4. Elija Launch instances (Lanzar instancias) y cree una instancia temporal en la misma zona de disponibilidad que la instancia afectada. Elija un tipo de instancia que use una versión de Windows diferente. Por ejemplo, si la instancia es Windows Server 2016, elija una instancia de Windows Server 2019.

   > **Important**
   >
   > Si no crea la instancia en la misma zona de disponibilidad que la instancia afectada, no podrá adjuntar el volumen raíz de la instancia afectada a la nueva instancia.

5. En el panel de navegación, elija Volumes (Volúmenes).
6. Localice el volumen raíz de la instancia afectada. Separe el volumen y adjúntelo a la instancia temporal que creó anteriormente. Adjúntelo con el nombre de dispositivo predeterminado (xvdf).
7. Utilice el Escritorio remoto para conectarse a la instancia temporal y, a continuación, utilice la utilidad de Administración de discos para hacer que el volumen esté disponible para su uso.

8. Abra el símbolo del sistema y ejecute el siguiente comando. Sustituya D por la letra de la unidad del volumen secundario que acaba de adjuntar:

```
bcdedit /store D:\Boot\BCD /set {default} safeboot dsrepair
```

9. En la utilidad de Administración de discos, elija la unidad que adjuntó anteriormente, abra el menú contextual (clic con el botón derecho) y elija Sin conexión.
10. En la consola de EC2, separe el volumen afectado de la instancia temporal y vuelva a adjuntarlo a la instancia original con el nombre de dispositivo `/dev/sda1`. Debe especificar este nombre de dispositivo para designar el volumen como volumen raíz.
11. Inicie la instancia.
12. Una vez que la instancia pase las comprobaciones de estado en la consola de EC2, conéctese a la instancia mediante el Escritorio remoto y compruebe si arranca en modo DSRM.
13. (Opcional) Elimine o detenga la instancia temporal que creó en este procedimiento.

La instancia pierde la conexión de red o las tareas programadas no se ejecutan como se espera

Si reinicia la instancia y pierde la conexión de red, es posible que la instancia tenga la hora incorrecta.

De manera predeterminada, las instancias de Windows usan la hora universal coordinada (UTC). Si establece la hora de la instancia en una zona horaria diferente y después la reinicia, la hora se desplaza y la instancia pierde temporalmente la dirección IP. La instancia recupera la conexión de red finalmente, pero puede llevar varias horas. La cantidad de tiempo que tarda la instancia en recuperar la conexión de red depende de la diferencia entre la hora UTC y la otra zona horaria.

Este mismo problema horario puede dar como resultado que las tareas programadas no se ejecuten cuando se espera. En este caso, las tareas programadas no se ejecutan como se espera porque la instancia tiene la hora incorrecta.

Para usar siempre una zona horaria distinta de UTC, debe establecer la clave del registro RealTimeIsUniversal. Sin esta clave, una instancia usa UTC después de reiniciarla.

Para solucionar los problemas de hora que provocan la pérdida de la conexión de red

1. Asegúrese de que está ejecutando los controladores PV recomendados. Para obtener más información, consulte the section called “Actualizar controladores PV”.

2. Compruebe que la siguiente clave del registro existe y que está establecida en 1: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation \RealTimeIsUniversal

No se puede obtener el resultado de la consola

Con las instancias de Windows, la consola de la instancia muestra el resultado de las tareas realizadas durante el proceso de arranque de Windows. Si Windows arranca correctamente, el último mensaje que se registra es `Windows is Ready to use`. También puede mostrar mensajes de registro de eventos en la consola, pero es posible que esta característica no esté habilitada de manera predeterminada, según la versión de Windows. Para obtener más información, consulte the section called “Configuración de agentes de inicialización de Windows”.

Para obtener la salida de la consola de la instancia utilizando la consola Amazon EC2, selecciona la instancia, luego selecciona Acciones, luego selecciona Supervisar y solucionar problemas y a continuación selecciona Obtener registro del sistema. Para obtener el resultado de la consola usando la línea de comandos, use uno de los comandos siguientes: get-console-output (AWS CLI) o Get-EC2ConsoleOutput (AWS Tools for Windows PowerShell).

En instancias que se ejecutan en Windows Server 2012 R2 y versiones anteriores, si el resultado de la consola está vacío, podría indicar un problema con el servicio EC2Config, como un archivo de configuración mal configurado o que Windows no arrancó correctamente. Para corregir este problema, descargue e instale la última versión de EC2Config. Para obtener más información, consulte the section called “Instalar EC2config”.

Windows Server 2012 R2 no está disponible en la red

Para obtener información acerca de la solución de problemas de una instancia de Windows Server 2012 R2 que no está disponible en la red, consulte Windows Server 2012 R2 pierde conectividad de red y almacenamiento después de reiniciar una instancia.

Colisión de firma de disco

Puede comprobar y resolver colisiones de firmas de disco mediante EC2Rescue for Windows Server. O bien, puede resolver manualmente los problemas de firma de disco si realiza los siguientes pasos:

> **Warning**
>
> En el siguiente procedimiento se describe cómo editar el Registro de Windows mediante el Editor del Registro. Si no está familiarizado con el Registro de Windows o cómo realizar cambios de forma segura mediante el Editor del Registro, consulte Configuración del Registro.

1. Abra un símbolo del sistema, escriba regedit.exe y, a continuación, presione Enter (Intro).
2. En el navegador Registry Editor (Editor del Registro), elija HKEY_LOCAL_MACHINE desde el menú contextual (haga clic con el botón derecho) y, luego, elija Find (Buscar).
3. Escriba Windows Boot Manager y, luego, elija Find Next (Buscar siguiente).
4. Elija la clave denominada `11000001`. Esta clave es un elemento secundario de la clave que encontró en el paso anterior.
5. En el panel derecho, elija `Element` y, a continuación, elija Modify (Modificar) desde el menú contextual (haga clic con el botón derecho).
6. Localice la firma del disco de cuatro bytes en el desplazamiento 0x38 en los datos. Esta es la firma de la base de datos de configuración de arranque (BCD). Invierta los bytes para crear la firma del disco y escríbalo. Por ejemplo, la firma de disco que se representa con los siguientes datos es `E9EB3AA5`:

   ```
   ...
   0030  00 00 00 00 01 00 00 00
   0038  A5 3A EB E9 00 00 00 00
   0040  00 00 00 00 00 00 00 00
   ...
   ```

7. En una ventana del símbolo del sistema, ejecute el siguiente comando para iniciar Microsoft DiskPart.

   ```
   diskpart
   ```

8. Ejecute el comando `select disk` DiskPart y especifique el número de disco para el volumen con la colisión de la firma del disco.

> **Tip**
>
> Para comprobar el número de disco del volumen con la colisión de firmas de disco, utilice la utilidad Administración de discos. Abra un símbolo del sistema, escriba `compmgmt.msc` y, a continuación, presione Enter. En el panel de navegación de la izquierda, haga doble clic en Administración de discos. En la utilidad Administración de discos, verifique el número de disco para el volumen fuera de línea con la colisión de la firma del disco.

```
DISKPART> select disk 1
Disk 1 is now the selected disk.
```

9. Ejecute el siguiente comando “DiskPart” para obtener la firma del disco.

```
DISKPART>  uniqueid disk
Disk ID: 0C764FA8
```

10. Si la firma del disco que se muestra en el paso anterior no coincide con la firma del disco que anotó anteriormente, use el siguiente comando DiskPart para cambiar la firma del disco para que coincida:

```
DISKPART> uniqueid disk id=E9EB3AA5
```

Mensajes comunes con instancias de Windows

En esta sección se incluyen sugerencias para solucionar problemas de mensajes comunes.

Mensajes

- "Password is not available"
- "Password not available yet"
- "Cannot retrieve Windows password"
- "Waiting for the metadata service"
- "Unable to activate Windows"
- "Windows is not genuine (0x80070005)"

- "No Terminal Server License Servers available to provide a license"
- "Tu organización administra algunas opciones de configuración"

"Password is not available"

Para conectarse a una instancia de Windows mediante el Escritorio remoto, debe especificar una cuenta y una contraseña. Las cuentas y las contraseñas proporcionadas se basan en la AMI que usó al lanzar la instancia. Puede recuperar la contraseña autogenerada para la cuenta de administrador o usar la cuenta y la contraseña que se usaron en la instancia original en la que se creó la AMI.

Puede generar una contraseña para la cuenta de administrador para las instancias lanzadas con una AMI de Windows personalizada. Para generar la contraseña, tendrá que configurar algunos ajustes en el sistema operativo antes de crear la AMI. Para obtener más información, consulte Creación de una AMI basada en Amazon EBS.

Si la instancia de Windows no está configurada para generar una contraseña aleatoria, recibirá el mensaje siguiente cuando recupere la contraseña autogenerada usando la consola:

```
Password is not available.
The instance was launched from a custom AMI, or the default password has changed. A
password cannot be retrieved for this instance. If you have forgotten your password,
 you can
reset it using the Amazon EC2 configuration service. For more information, see
 Passwords for a
Windows Server instance.
```

Compruebe el resultado de la consola para la instancia para ver si la AMI que usó para lanzarla se creó con la generación de contraseñas deshabilitada. Si la generación de contraseñas está deshabilitada, el resultado de la consola contiene lo siguiente:

```
Ec2SetPassword: Disabled
```

Si la generación de contraseñas está deshabilitada y no recuerda la contraseña de la instancia original, puede restablecerla para esta instancia. Para obtener más información, consulte Restablecer una contraseña de administrador de Windows perdida o vencida.

"Password not available yet"

Para conectarse a una instancia de Windows mediante el Escritorio remoto, debe especificar una cuenta y una contraseña. Las cuentas y las contraseñas proporcionadas se basan en la AMI que usó al lanzar la instancia. Puede recuperar la contraseña autogenerada para la cuenta de administrador o usar la cuenta y la contraseña que se usaron en la instancia original en la que se creó la AMI.

La contraseña debería estar disponible en unos minutos. Si la contraseña no está disponible, recibirá el mensaje siguiente cuando recupere la contraseña autogenerada usando la consola:

```
Password not available yet.
Please wait at least 4 minutes after launching an instance before trying to retrieve
 the
auto-generated password.
```

Si han pasado más de cuatro minutos y sigue sin obtener la contraseña, es posible que el agente de lanzamiento de la instancia no esté configurado para generar una contraseña. Verifíquelo comprobando si el resultado de la consola está vacío. Para obtener más información, consulte No se puede obtener el resultado de la consola.

Compruebe también que la cuenta de AWS Identity and Access Management (IAM) utilizada para acceder al Portal de administración permita la acción `ec2:GetPasswordData`. Para obtener más información sobre los permisos de IAM, consulte What is IAM?

"Cannot retrieve Windows password"

Para recuperar la contraseña autogenerada de la cuenta de administrador, debe usar la clave privada del par de claves que especificó cuando lanzó la instancia. Si no especificó un par de claves al lanzar la instancia, recibirá el mensaje siguiente.

```
Cannot retrieve Windows password
```

Puede terminar la instancia y lanzar una nueva usando la misma AMI y asegurándose de que especifica un par de claves.

"Waiting for the metadata service"

Una instancia de Windows debe obtener información de los metadatos de la instancia para poder activarse. De manera predeterminada, el valor `WaitForMetaDataAvailable` asegura que el servicio EC2Config espera a que los metadatos de la instancia sean accesibles antes de continuar

con el proceso de arranque. Para obtener más información, consulte Trabajar con metadatos de instancias.

Si la instancia no supera la prueba de accesibilidad, intente lo siguiente para solucionar el problema.

- Compruebe el bloque de CIDR de la VPC. Las instancias de Windows no se podrán iniciar correctamente si se lanzan en una VPC con un rango de direcciones IP de `224.0.0.0` a `255.255.255.255` (rangos de direcciones IP de clase D y clase E). Estos rangos de direcciones IP están reservados y no deberían asignarse a los dispositivos host. Recomendamos que cree una VPC con un bloque de CIDR de los rangos de direcciones IP privadas (no enrutables públicamente) como se especifica en RFC 1918.
- Es posible que el sistema se haya configurado con una dirección IP estática. Pruebe a crear una interfaz de red y a asociarla a la instancia.
- Para habilitar DHCP en una instancia de Windows con la que no se puede conectar

  1. Detenga la instancia afectada y sepárela del volumen raíz.
  2. Lance una instancia temporal en la misma zona de disponibilidad que la instancia afectada.

     > **Warning**
     >
     > Si la instancia temporal se basa en la misma AMI que la instancia original, debe completar otros pasos o no podrá arrancar la instancia original después de restaurar el volumen raíz debido a un conflicto de firmas de disco. Como alternativa, selecciones una AMI diferente para la instancia temporal. Por ejemplo, si la instancia original utiliza una AMI de Windows de AWS para Windows Server 2016, lance la instancia temporal mediante el uso de una AMI de Windows de AWS para Windows Server 2019.

  3. Adjunte el volumen raíz de la instancia afectada a esta instancia temporal. Conéctese a la instancia temporal, abra la utilidad Administración de discos y ponga la unidad online.
  4. En la instancia temporal, abra Regedit y seleccione HKEY_LOCAL_MACHINE. En el menú Archivo, elija Cargar Hive. Seleccione la unidad, abra el archivo `Windows\System32\config\SYSTEM` y especifique un nombre de clave cuando se solicite (puede usar cualquier nombre).
  5. Seleccione la clave que acaba de cargar y desplácese hasta `ControlSet001\Services\Tcpip\Parameters\Interfaces`. Cada interfaz de red la enumera un GUID. Seleccione la interfaz de red correcta. Si DHCP está deshabilitado y hay una dirección IP estática asignada, `EnableDHCP` se establece en 0. Para habilitar DHCP, establezca `EnableDHCP`

en 1 y elimine las siguientes claves si existen: `NameServer`, `SubnetMask`, `IPAddress` y `DefaultGateway`. Seleccione la clave de nuevo y en el menú Archivo, elija Descargar Hive.

> **Note**
>
> Si tiene varias interfaces de red, tendrá que identificar la correcta para habilitar DHCP. Para identificar la interfaz de red correcta, revise los siguientes valores `NameServer`, `SubnetMask`, `IPAddress` y `DefaultGateway`. Estos valores muestran la configuración estática de la instancia previa.

6. (Opcional) Si DHCP ya está habilitado, es posible que no tenga una ruta al servicio de metadatos. Actualizar EC2Config puede resolver este problema.

   a. Descargue e instale la última versión del servicio EC2Config. Para obtener más información sobre cómo instalar este servicio, consulte the section called “Instalar EC2config”.

   b. Extraiga los archivos del archivo `.zip` en el directorio `Temp` de la unidad que ha adjuntado.

   c. Abra Regedit y seleccione HKEY_LOCAL_MACHINE. En el menú Archivo, elija Cargar Hive. Seleccione la unidad, abra el archivo `Windows\System32\config\SOFTWARE` y especifique un nombre de clave cuando se solicite (puede usar cualquier nombre).

   d. Seleccione la clave que acaba de cargar y desplácese hasta `Microsoft\Windows\CurrentVersion`. Seleccione la clave `RunOnce`. (Si esta clave no existe, haga clic con el botón derecho en `CurrentVersion`, seleccione Nuevo, Clave y asigne a la clave el nombre `RunOnce`). Haga clic con el botón derecho, seleccione Nuevo y elija Valor de cadena. Escriba `Ec2Install` como nombre y `C:\Temp\Ec2Install.exe -q` como dato.

   e. Seleccione la clave de nuevo y en el menú Archivo, elija Descargar Hive.

7. (Opcional) Si la instancia temporal se basa en la misma AMI que la instancia original, debe completar los siguientes pasos o no podrá arrancar la instancia original después de restaurar el volumen raíz debido a un conflicto de firmas de disco.

> **Warning**
>
> En el siguiente procedimiento se describe cómo editar el Registro de Windows mediante el Editor del Registro. Si no está familiarizado con el Registro de Windows

o cómo realizar cambios de forma segura mediante el Editor del Registro, consulte Configuración del Registro.

a. Abra un símbolo del sistema, escriba regedit.exe y, a continuación, presione Enter (Intro).

b. En el navegador Registry Editor (Editor del Registro), elija HKEY_LOCAL_MACHINE desde el menú contextual (haga clic con el botón derecho) y, luego, elija Find (Buscar).

c. Escriba Windows Boot Manager y, luego, elija Find Next (Buscar siguiente).

d. Elija la clave denominada `11000001`. Esta clave es un elemento secundario de la clave que encontró en el paso anterior.

e. En el panel derecho, elija `Element` y, a continuación, elija Modify (Modificar) desde el menú contextual (haga clic con el botón derecho).

f. Localice la firma del disco de cuatro bytes en el desplazamiento 0x38 en los datos. Invierta los bytes para crear la firma del disco y escríbalo. Por ejemplo, la firma de disco que se representa con los siguientes datos es `E9EB3AA5`:

```
...
0030  00 00 00 00 01 00 00 00
0038  A5 3A EB E9 00 00 00 00
0040  00 00 00 00 00 00 00 00
...
```

g. En una ventana del símbolo del sistema, ejecute el siguiente comando para iniciar Microsoft DiskPart.

```
diskpart
```

h. Ejecute el siguiente comando “DiskPart” para seleccionar el volumen. (Puede verificar que el número de disco es 1 mediante la utilidad Administración de discos).

```
DISKPART> select disk 1

Disk 1 is now the selected disk.
```

i. Ejecute el siguiente comando “DiskPart” para obtener la firma del disco.

```
DISKPART>  uniqueid disk
```

```
Disk ID: 0C764FA8
```

j. Si la firma de disco que se muestra en el paso anterior no coincide con la del disco de BCD que escribió anteriormente, utilice el siguiente comando “DiskPart” para cambiar la firma de disco de manera que coincida:

```
DISKPART> uniqueid disk id=E9EB3AA5
```

8. Use la utilidad Administración de discos para desconectar la unidad.

> **Note**
>
> La unidad queda automáticamente sin conexión si la instancia temporal ejecuta el mismo sistema operativo que la instancia afectada, por lo que no tendrá que desconectarla manualmente.

9. Separe el volumen de la instancia temporal. Puede terminar la instancia temporal si no va a utilizarla más.
10. Restaure el volumen raíz de la instancia afectada adjuntando el volumen como `/dev/sda1`.
11. Inicie la instancia afectada.

Si se ha conectado a la instancia, abra un explorador de Internet desde la instancia y escriba la siguiente URL del servidor de metadatos:

```
http://169.254.169.254/latest/meta-data/
```

Si no puede contactar con el servidor de metadatos, intente lo siguiente para resolver el problema:

- Descargue e instale la última versión del servicio EC2Config. Para obtener más información sobre cómo instalar este servicio, consulte the section called “Instalar EC2config”.
- Compruebe si la instancia de Windows está ejecutando los controladores PV de RedHat. Si es así, actualice a los controladores PV de Citrix. Para obtener más información, consulte the section called “Actualizar controladores PV”.
- Verifique que las configuraciones de firewall, IPSec y proxy no bloquean el tráfico saliente al servicio de metadatos (`169.254.169.254`) o a los servidores AWS KMS (las direcciones se especifican en los elementos de `TargetKMSServer` en `C:\Program Files\Amazon\Ec2ConfigService\Settings\ActivationSettings.xml`).

- Verifique que tiene la ruta al servicio de metadatos (`169.254.169.254`) con el comando siguiente.

```
route print
```

- Compruebe los problemas de red que puedan afectar a la zona de disponibilidad de la instancia. Vaya a http://status.aws.amazon.com/.

"Unable to activate Windows"

Las instancias de Windows usan la activación de AWS KMS de Windows. Puede recibir este mensaje: `A problem occurred when Windows tried to activate. Error Code 0xC004F074` si la instancia no puede alcanzar el servidor AWS KMS. Windows debe activarse cada 180 días. EC2Config intenta contactar con el servidor AWS KMS antes de que termine el periodo de activación para asegurar que Windows se mantiene activado.

Si se produce un problema de activación de Windows, use el procedimiento siguiente para resolverlo.

Para EC2Config (AMI de Windows Server 2012 R2 y anteriores)

1. Descargue e instale la última versión del servicio EC2Config. Para obtener más información sobre cómo instalar este servicio, consulte the section called “Instalar EC2config”.
2. Inicie sesión en la instancia y abra el archivo siguiente: `C:\Program Files\Amazon\Ec2ConfigService\Settings\config.xml`.
3. Localice el complemento Ec2WindowsActivate en el archivo `config.xml`. Cambie el estado a Enabled (Habilitado) y guarde los cambios.
4. En el complemento Windows Services, reinicie el servicio EC2Config o reinicie la instancia.

Si no se resuelve el problema de activación, siga estos otros pasos adicionales.

1. Establezca el AWS KMS de destino: C:\> slmgr.vbs /skms 169.254.169.250:1688
2. Active Windows: C:\> slmgr.vbs /ato

Para EC2Launch (AMI de Windows Server 2016 y anteriores)

1. Desde un símbolo de PowerShell con derechos administrativos, importa el módulo EC2Launch:

```
PS C:\> Import-Module "C:\ProgramData\Amazon\EC2-Windows\Launch\Module
\Ec2Launch.psd1"
```

2. Llama la función Add-Routes para ver la lista de rutas nuevas:

```
PS C:\> Add-Routes
```

3. Llame a la función Set-ActivationSettings:

```
PS C:\> Set-Activationsettings
```

4. A continuación, ejecute el script siguiente para activar Windows:

```
PS C:\> cscript "${env:SYSTEMROOT}\system32\slmgr.vbs" /ato
```

Tanto para EC2Config como EC2Launch, si continúa recibiendo un error de activación, verifique la información siguiente.

- Verifique que tiene rutas a los servidores AWS KMS. Abra `C:\Program Files\Amazon\Ec2ConfigService\Settings\ActivationSettings.xml` y localice los elementos `TargetKMSServer`. Ejecute el comando siguiente y compruebe si aparecen las direcciones de estos servidores AWS KMS.

```
route print
```

- Compruebe que la clave del cliente de AWS KMS está establecida. Ejecute el siguiente comando y compruebe el resultado.

```
C:\Windows\System32\slmgr.vbs /dlv
```

  Si el resultado contiene Error: product key not found, la clave del cliente de AWS KMS no está establecida. Si la clave del cliente de AWS KMS no está establecida, busque la clave del cliente según se describe en este artículo de Microsoft: AWS KMS Client Setup Keys y, a continuación, ejecute el comando siguiente para establecer la clave del cliente de AWS KMS.

```
C:\Windows\System32\slmgr.vbs /ipk client_key
```

- Verifique que el sistema tiene la hora y la zona horaria correctas. Si utiliza una zona horaria distinta de UTC, agregue la siguiente clave de registro y configúrela en 1 para asegurarse de que la hora es correcta: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\RealTimeIsUniversal`.
- Si Windows Firewall está habilitado, deshabilítelo temporalmente con el comando siguiente.

```
netsh advfirewall set allprofiles state off
```

"Windows is not genuine (0x80070005)"

Las instancias de Windows usan la activación de AWS KMS de Windows. Si una instancia no puede completar el proceso de activación, informa de que la copia de Windows no es auténtica.

Intente las sugerencias de "Unable to activate Windows".

"No Terminal Server License Servers available to provide a license"

De manera predeterminada, Windows Server tiene licencia para dos usuarios simultáneos a través de Escritorio remoto. Si necesita proporcionar acceso simultáneo a más de dos usuarios a la instancia de Windows a través de Escritorio remoto, puede comprar una licencia de acceso de cliente (CAL) para los servicios de Escritorio remoto e instalar los roles de servidor de licencias de Escritorio remoto y host de sesión de Escritorio remoto.

Compruebe los problemas siguientes:

- Ha superado el número máximo de sesiones RDP simultáneas.
- Ha instalado el rol de servicio Escritorio remoto de Windows.
- La licencia ha caducado. Si la licencia ha caducado, no puede conectar con la instancia de Windows como usuario. Puede intentar lo siguiente:
  - Conéctese a la instancia desde la línea de comandos usando un parámetro `/admin`, por ejemplo:

    ```
    mstsc /v:instance /admin
    ```

    Para obtener más información, consulte el siguiente artículo de Microsoft: Access Remote Desktop Via Command Line.

- Detenga la instancia, separe sus volúmenes de Amazon EBS y adjúntelos a otra instancia de la misma zona de disponibilidad para recuperar los datos.

”Tu organización administra algunas opciones de configuración”

En las instancias lanzadas desde las AMI de Windows Server más recientes, podría aparecer el siguiente mensaje de Windows Update: "Tu organización administra algunas opciones de configuración". Este mensaje aparece por algunos cambios realizados en Windows Server y no afecta al comportamiento de Windows Update o a su capacidad de administrar la configuración de la actualización.

Para eliminar esta advertencia

1. Abra `gpedit.msc` y acceda a Computer Configuration (Configuración del equipo), Administrative Templates (Plantillas administrativas), Windows Components (Componentes de Windows) y Windows updates (Actualizaciones de Windows). Edite Configure Automatic Update (Configurar actualización automática) y establezca esta opción en enabled (habilitada).
2. En una ventana del símbolo del sistema, actualice la política de grupo mediante gpupdate /force.
3. Cierre y vuelva a abrir la Configuración de actualizaciones de Windows. Verá el mensaje anterior acerca de que su organización administra la configuración, seguido de «Descargaremos las actualizaciones automáticamente, excepto en conexiones de uso medido (donde se podrían aplicar cargos). En tal caso, descargaremos automáticamente estas actualizaciones requeridas para que Windows siga funcionando sin problemas”.
4. Vuelva a `gpedit.msc` y establezca de nuevo la directiva de grupo en not configured (no configurada). Vuelva a ejecutar gpupdate /force.
5. Cierre el símbolo del sistema y espere unos minutos.
6. Vuelva a abrir la Configuración de actualizaciones de Windows. No debería aparecer el mensaje ”Tu organización administra algunas opciones de configuración”.

Solucionar problemas de lanzamiento de instancias

Los siguientes problemas impiden lanzar una instancia.

Problemas de lanzamiento

- Nombre de dispositivo no válido

- Límite de la instancia excedido
- Capacidad de la instancia insuficiente
- La configuración solicitada no se admite actualmente. Consulte la documentación para ver las configuraciones admitidas.
- La instancia termina inmediatamente
- Permisos insuficientes
- Elevado uso de la CPU justo después de iniciar Windows (instancias de Windows únicamente)

Nombre de dispositivo no válido

Descripción

Se obtiene el error `Invalid device name` *`device_name`* cuando se intenta lanzar una instancia nueva.

Causa

Si aparece este error cuando intenta lanzar una instancia, el nombre de dispositivo especificado para uno o más volúmenes en la solicitud no es válido. Entre las causas posibles se incluyen las siguientes:

- Es posible que la AMI seleccionada esté utilizando el nombre del dispositivo.
- Es posible que el nombre del dispositivo esté reservado para los volúmenes raíz.
- Es posible que el nombre del dispositivo se utilice para otro volumen de la solicitud.
- Es posible que el nombre del dispositivo no sea válido para el sistema operativo.

Solución

Para resolver el problema:

- Asegúrese de que el nombre del dispositivo no se utilice en la AMI que seleccionó. Ejecute el siguiente comando para ver los nombres de dispositivos que utiliza la AMI.

```
aws ec2 describe-images --image-id ami_id --query
 'Images[*].BlockDeviceMappings[].DeviceName'
```

- Asegúrese de no utilizar un nombre de dispositivo que esté reservado para los volúmenes raíz. Para obtener más información, consulte Nombres de dispositivos disponibles.
- Asegúrese de que cada volumen especificado en la solicitud tenga un nombre de dispositivo único.
- Asegúrese de que los nombres de los dispositivos que especificó tengan el formato correcto. Para obtener más información, consulte Nombres de dispositivos disponibles.

Límite de la instancia excedido

Descripción

Se obtiene el error `InstanceLimitExceeded` cuando se intenta lanzar una nueva instancia o reiniciar una instancia parada.

Causa

Si recibe un error `InstanceLimitExceeded` cuando intenta lanzar una nueva instancia o reiniciar una instancia detenida, ha alcanzado el límite en el número de instancias que puede lanzar en una región. Cuando crea la cuenta de AWS, establecemos los límites predeterminados en el número de instancias que puede ejecutar por región.

Solución

Puede solicitar un aumento de límite de instancias por región. Para obtener más información, consulte Cuotas de servicio de Amazon EC2.

Capacidad de la instancia insuficiente

Descripción

Se obtiene el error `InsufficientInstanceCapacity` cuando se intenta lanzar una nueva instancia o reiniciar una instancia parada.

Causa

Si recibe este error cuando intenta lanzar la instancia o reiniciar una instancia detenida, AWS no tiene actualmente capacidad bajo demanda disponible para llevar a cabo la solicitud.

Solución

Para resolver este problema, pruebe lo siguiente:

- Espere unos minutos y después envíe la solicitud de nuevo; la capacidad puede cambiar frecuentemente.
- Envíe una nueva solicitud con una cantidad reducida de instancias. Por ejemplo, si hace una única solicitud para lanzar 15 instancias, intente hacer 3 solicitudes para 5 instancias, o 15 solicitudes para 1 instancia en su lugar.
- Si está lanzando una instancia, envíe una nueva solicitud sin especificar ninguna zona de disponibilidad.
- Si está lanzando una instancia, envíe una nueva solicitud usando un tipo de instancia distinto (que puede cambiar de tamaño en una fase posterior). Para obtener más información, consulte Cambie el tipo de instancia.
- Si está lanzando instancias en un grupo de ubicación en clúster, es posible que reciba un error de capacidad insuficiente. Para obtener más información, consulte Trabajo con grupos con ubicación.

La configuración solicitada no se admite actualmente. Consulte la documentación para ver las configuraciones admitidas.

Descripción

Recibe el error `Unsupported` cuando intenta lanzar una nueva instancia porque la configuración de la instancia no es compatible.

Causa

El mensaje de error proporciona detalles adicionales. Por ejemplo, es posible que no se admita un tipo de instancia o una opción de compra de instancia en la región o zona de disponibilidad especificadas.

Solución

Pruebe una configuración de instancia diferente. Para buscar un tipo de instancia que cumpla sus requisitos, consulte Búsqueda de un tipo de instancia de Amazon EC2.

La instancia termina inmediatamente

Descripción

La instancia pasa del estado `pending` al estado `terminated`.

Causa

A continuación se ofrecen unas cuantas razones sobre por qué una instancia puede terminar de inmediato:

- Ha superado los límites de volumen de EBS. Para obtener más información, consulte Límites de volumen de instancias.
- Una instantánea de EBS está dañada.
- El volumen de EBS raíz está cifrado y no tiene permiso para acceder a la Clave de KMS para descifrarlo.
- Hay una instantánea especificada en la asignación de dispositivos de bloque de la AMI que está cifrada y no tiene permiso para acceder a la Clave de KMS para descifrarla, o no tiene acceso a la Clave de KMS para cifrar los volúmenes restaurados.
- A la AMI con respaldo en el almacén de instancias que utilizaba para lanzar la instancia le falta una parte obligatoria (un archivo image.part.xx).

Para obtener más información, obtenga el motivo de terminación utilizando uno de los métodos siguientes.

Para obtener el motivo de la terminación utilizando la consola de Amazon EC2

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instances (Instancias) y seleccione la instancia.
3. En la primera pestaña, busque el motivo junto a State transition reason (Motivo de transición de estado).

Para obtener el motivo de la terminación utilizando la consola de AWS Command Line Interface

1. Use el comando describe-instances y especifique el ID de instancia.

   ```
   aws ec2 describe-instances --instance-id instance_id
   ```

2. Revise la respuesta JSON devuelta por el comando y anote los valores en el elemento de respuesta `StateReason`.

   En el siguiente bloque de código se muestra un ejemplo de un elemento de respuesta `StateReason`.

```
"StateReason": {
  "Message": "Client.VolumeLimitExceeded: Volume limit exceeded",
  "Code": "Server.InternalError"
},
```

Para obtener el motivo de terminación utilizando la consola de AWS CloudTrail

Para obtener más información, consulte Ver eventos con el historial de eventos de CloudTrail en la Guía del usuario de AWS CloudTrail.

Solución

En función del motivo de terminación, realice una de las siguientes operaciones:

- **`Client.VolumeLimitExceeded: Volume limit exceeded`** — elimine los volúmenes que no estén en uso. Puede enviar una solicitud para aumentar el límite del volumen.
- **`Client.InternalError: Client error on launch`** — asegúrese de que tiene los permisos necesarios para acceder a las AWS KMS keys que se utilizan para cifrar y descifrar volúmenes. Para obtener más información, consulte Uso de políticas de claves en AWS KMS en la Guía para desarrolladores de AWS Key Management Service.

Permisos insuficientes

Descripción

Obtiene el error `"errorMessage": "You are not authorized to perform this operation."` cuando intenta iniciar una nueva instancia y el inicio falla.

Causa

Si recibe este error al intentar lanzar una instancia, significa que no tiene los permisos de IAM necesarios para lanzarla.

Los posibles permisos faltantes incluyen:

- `ec2:RunInstances`
- `iam:PassRole`

Es posible que también falten otros permisos. Para obtener la lista de permisos necesarios para lanzar una instancia, consulte los ejemplos de políticas de IAM en Ejemplo: uso del asistente de inicialización de instancias de EC2 y Iniciar instancias (RunInstances).

Solución

Para resolver el problema:

- Si realiza las solicitudes como usuario de IAM, compruebe que los siguientes permisos se cumplan:
  - `ec2:RunInstances` con un recurso de comodín ("*")
  - `iam:PassRole` con el recurso que coincide con el ARN del rol (por ejemplo, `arn:aws:iam::999999999999:role/ExampleRoleName`)
- Si no tiene los permisos anteriores, edite la política de IAM asociada al rol o usuario de IAM para agregar los permisos necesarios que faltan.

Si el problema no se resuelve y sigue recibiendo un error de error de lanzamiento, puede decodificar el mensaje de error de autorización incluido en el error. El mensaje decodificado incluye los permisos que faltan en la política de IAM. Para obtener más información, consulte ¿Cómo puedo decodificar un mensaje de error de autorización después de recibir un error de “UnauthorizedOperation” durante el inicio de una instancia de EC2?

Elevado uso de la CPU justo después de iniciar Windows (instancias de Windows únicamente)

> **Note**
>
> Este consejo de solución de problemas es solo para instancias de Windows.

Si Windows Update está establecido en Buscar actualizaciones, pero permitirme elegir si deseo descargarlas e instalarlas (el valor predeterminado de la instancia) esta comprobación puede consumir entre un 50 y un 99 % de la CPU de la instancia. Si este consumo de la CPU causa problemas en las aplicaciones, puede cambiar manualmente la configuración de Windows Update en el Panel de control o puede usar el script siguiente en el campo de datos de usuario de Amazon EC2:

```
reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update" /v
 AUOptions /t REG_DWORD /d 3 /f net stop wuauserv net start wuauserv
```

Cuando ejecute este script, especifique un valor para /d. El valor predeterminado es 3. Entre los valores posibles se incluyen:

1. Nunca buscar actualizaciones
2. Buscar actualizaciones, pero permitirme elegir si deseo descargarlas e instalarlas
3. Descargar actualizaciones, pero permitirme elegir si deseo instalarlas
4. Instalar actualizaciones automáticamente

Después de modificar los datos de usuario para la instancia, puede ejecutarla. Para obtener más información, consulte Ejecutar comandos en la instancia de Windows en la inicialización.

Solución de problemas de conexión a la instancia de Linux

La información y errores comunes que se presentan a continuación pueden ayudarle a solucionar problemas relacionados con la conexión a la instancia de Linux.

Problemas de conectividad

- Causas comunes de problemas de conexión
- Error connecting to your instance: Connection timed out
- Error: no se puede cargar la clave... Se espera: CUALQUIER CLAVE PRIVADA
- Error: User key not recognized by server
- Error: Permiso denegado o conexión cerrada por [instancia] puerto 22
- Error: Unprotected Private Key File (Error: archivo de clave privada no protegido)
- Error: La clave privada debe empezar por "-----BEGIN RSA PRIVATE KEY-----" y terminar por "-----END RSA PRIVATE KEY-----"
- Error: Server refused our key o No supported authentication methods available
- Cannot Ping Instance (No se puede ejecutar Ping en la instancia)
- Error: el servidor ha cerrado inesperadamente la conexión de red
- Error: no se pudo validar la clave de host para EC2 Instance Connect
- No es posible conectarse a la instancia Ubuntu mediante EC2 Instance Connect

- Perdí mi clave privada. ¿Cómo puedo conectarme a mi instancia de Linux?

Causas comunes de problemas de conexión

Le recomendamos que para solucionar los problemas de conexión a instancias compruebe que ha realizado correctamente las siguientes tareas.

Compruebe el nombre de usuario de su instancia

Puede conectarse a la instancia mediante el nombre de usuario de su cuenta de usuario o el nombre de usuario predeterminado de la AMI que utilizó para lanzar la instancia.

- Obtener el nombre de usuario de su cuenta de usuario.

  Para obtener más información sobre cómo crear una cuenta de usuario, consulte Administración de usuarios del sistema en la instancia de Linux.
- Obtenga el nombre de usuario predeterminado para la AMI que utilizó para iniciar la instancia:

AMI utilizada para iniciar la instancia.	Nombre de usuario predeterminado
AL2023 Amazon Linux 2 Amazon Linux	`ec2-user`
CentOS	`centos` o `ec2-user`
Debian	`admin`
Fedora	`fedora` o `ec2-user`
RHEL	`ec2-user` o `root`
SUSE	`ec2-user` o `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`

AMI utilizada para iniciar la instancia.	Nombre de usuario predeterminado
Rocky Linux	`rocky`
Otro	Comprobación con el proveedor de AMI

Compruebe que las reglas del grupo de seguridad permiten tráfico

Asegúrese de que el grupo de seguridad asociado a la instancia permita el tráfico SSH que ingresa desde la dirección IP. El grupo de seguridad predeterminado de la VPC no permite el tráfico SSH entrante de forma predeterminada. El grupo de seguridad creado por el Launch Wizard de instancias habilita el tráfico SSH de forma predeterminada. Para ver los pasos para agregar una regla para el tráfico de SSH entrante a su instancia de Linux, consulte Reglas para conectarse a las instancias desde un equipo. Para ver los pasos para realizar la comprobación, consulte Error connecting to your instance: Connection timed out.

Verifique que la instancia esté lista

Una vez lanzada la instancia, pueden transcurrir unos minutos hasta que esté lista para conectarse. Compruebe su instancia para asegurarse de que se está ejecutando y ha superado sus comprobaciones de estado.

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instances (Instancias) y seleccione la instancia.
3. Compruebe lo siguiente:

    a. En la columna Instance state (Estado de instancia), compruebe que la instancia esté en el estado `running`.
    b. En la columna Status check (Comprobación de estado), compruebe que la instancia haya superado las dos comprobaciones de estado.

Compruebe que haya cumplido con todos los requisitos previos para conectarse.

Asegúrese de tener toda la información que necesita para conectarse. Para obtener más información, consulte Conexión con la instancia de Linux.

Para obtener información sobre los requisitos previos específicos de los tipos de conexión, como SSH, EC2 Instance Connect, OpenSSH, PuTTY y más, consulte las siguientes opciones.

Linux o macOS X

Si el sistema operativo del equipo local es Linux o macOS X, compruebe los requisitos previos específicos para las siguientes opciones de conexión:

- Cliente SSH
- Conexión de instancia EC2
- Administrador de sesiones de AWS Systems Manager

Windows

Si el sistema operativo del equipo local es Windows, compruebe los requisitos previos específicos para las siguientes opciones de conexión:

- OpenSSH
- PuTTY
- Administrador de sesiones de AWS Systems Manager
- Windows Subsystem for Linux

Error connecting to your instance: Connection timed out

Si intenta conectarse a la instancia y recibe el mensaje de error `Network error: Connection timed out` o `Error connecting to [instance], reason: -> Connection timed out: connect`, pruebe lo siguiente:

Compruebe las reglas del grupo de seguridad.

Necesita un grupo de seguridad que permita el tráfico de entrada de la dirección IPv4 pública en el puerto adecuado.

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instances (Instancias) y seleccione la instancia.
3. En la ficha Security (Seguridad) de la parte inferior de la página de la consola, debajo de Inbound rules (Reglas de entrada), compruebe la lista de reglas efectivas para la instancia seleccionada.

   - En instancias de Linux: compruebe que hay una regla que permite el tráfico desde el equipo hasta el puerto 22 (SSH).
   - En instancias de Windows: compruebe que hay una regla que permite el tráfico desde el equipo hasta el puerto 3389 (RDP).

Si su grupo de seguridad no tiene una regla que permita el tráfico entrante desde su ordenador local, agregue una regla a su grupo de seguridad. Para obtener más información, consulte Reglas para conectarse a las instancias desde un equipo.

4. Para ver la regla que permite el tráfico entrante, consulte el campo Source (Fuente). Si el valor es una sola dirección IP y si la dirección IP no es estática, se asignará una nueva dirección IP cada vez que reinicie el equipo. Esto hará que la regla no incluya el tráfico de la dirección IP de su equipo. La dirección IP puede no ser estática si el equipo se encuentra en una red corporativa, si se conecta mediante un proveedor de servicios de Internet (ISP), o si la dirección IP de su equipo es dinámica y cambia cada vez que se reinicia el equipo. Para garantizar que la regla de grupo de seguridad permita el tráfico entrante desde el equipo local, en lugar de especificar una sola dirección IP para Source (Fuente), en su lugar, especifique el rango de direcciones IP que utilizan los equipos cliente.

   Si desea obtener más información acerca de las reglas del grupo de seguridad, consulte Security group rules (Reglas del grupo de seguridad) en la Guía del usuario de Amazon VPC.

Compruebe la tabla de ruteo de la subred.

Necesita una ruta que envíe todo el tráfico destinado fuera de la VPC al gateway de Internet para la VPC.

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instances (Instancias) y seleccione la instancia.
3. En la ficha Networking (Redes), tome nota de los valores del ID de VPC y el ID de subred.
4. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
5. En el panel de navegación, elija Internet Gateways (Gateways de Internet). Verifique que hay una gateway de Internet adjunta a la VPC. De lo contrario, elija Create internet gateway (Crear gateway de Internet), escriba un nombre para la gateway de Internet y elija Create internet gateway (Crear gateway de Internet). A continuación, para la gateway de Internet que creó, elija Actions (Acciones), Attach to VPC (Conectar a VPC), seleccione la VPC y, a continuación, elija Attach internet gateway (Conectar gateway de Internet) para conectarla a la VPC.
6. En el panel de navegación, elija Subnets (Subredes) y, a continuación, seleccione la suya.
7. En la pestaña Route Table (Tabla de ruteo), verifique que haya una ruta con `0.0.0.0/0` como destino y la gateway de Internet de la VPC como destino. Si está conectando con la instancia

utilizando la dirección IPv6, verifique que existe una ruta para todo el tráfico IPv6 (`::/0`) que apunte a la gateway de Internet. De lo contrario, realice lo siguiente:

a. Elija el ID de la tabla de ruteo (rtb-xxxxxxxx) para navegar a la tabla de ruteo.
b. En la pestaña Routes (Rutas), elija Edit routes (Editar rutas). Elija Add route (Añadir ruta) y utilice `0.0.0.0/0` como destino y la gateway de Internet como objetivo. Para IPv6, elija Add route (Añadir ruta) y utilice `::/0` como destino y la gateway de Internet como objetivo.
c. Elija Save routes (Guardar rutas).

Compruebe la lista de control de acceso (ACL) a la red para la subred.

Las ACL de red deben permitir el tráfico entrante desde su dirección IP local a través del puerto 22 (para las instancias de Linux) o del puerto 3389 (para las instancias de Windows). También deben permitir el tráfico saliente que se dirija a los puertos efímeros (1024-65535).

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.
4. En la pestaña Network ACL (ACL de red), en Inbound rules (Reglas de entrada), verifique que las reglas permitan el tráfico entrante desde su computadora a través del puerto requerido. Si no es así, elimine o modifique la regla que esté bloqueando el tráfico.
5. En Outbound rules (Reglas de salida), verifique que las reglas permitan el tráfico saliente hacia su equipo a través de los puertos efímeros. Si no es así, elimine o modifique la regla que esté bloqueando el tráfico.

Si el equipo está en una red corporativa,

pregunte al administrador de red si el firewall interno permite el tráfico de entrada y salida del equipo en el puerto 22 (para instancias de Linux) o el puerto 3389 (para instancias de Windows).

Si tiene un firewall en el equipo, compruebe que permite el tráfico de entrada y salida del equipo en el puerto 22 (para las instancias de Linux) o el puerto 3389 (para instancias de Windows).

Compruebe que la instancia tiene una dirección IPv4 pública.

Si no, asocie una dirección IP elástica a su instancia. Para obtener más información, consulte Direcciones IP elásticas.

Compruebe la carga de la CPU en la instancia; el servidor puede estar sobrecargado.

AWS proporciona de forma automática datos como las métricas y el estado de la instancia de Amazon CloudWatch, que puede utilizar para comprobar cuánta carga de la CPU está en la instancia y, si es necesario, ajustar cómo se controlan las cargas. Para obtener más información, consulte Monitorear las instancias con CloudWatch.

- Si la carga es variable, puede escalar automáticamente las instancias hacia arriba o hacia abajo utilizando Auto Scaling y Elastic Load Balancing.
- Si la carga crece de forma uniforme, puede pasar a un tipo de instancia mayor. Para obtener más información, consulte Cambie el tipo de instancia.

Para conectarse con la instancia a través de la dirección IPv6, compruebe lo siguiente:

- La subred debe estar asociada a una tabla de ruteo que tenga una ruta para el tráfico IPv6 (`::/0`) a una gateway de Internet.
- Las reglas del grupo de seguridad deben permitir el tráfico de la dirección IPv6 local en el puerto adecuado (22 para Linux y 3389 para Windows).
- Las reglas ACL de la red deben permitir el tráfico IPv6 de entrada y salida.
- Si lanzó la instancia desde una AMI más antigua, tal vez no esté configurada para DHCPv6 (las direcciones IPv6 no se reconocen automáticamente en la interfaz de red). Para obtener más información, consulte Configure IPv6 on your instances (Configuración de IPv6 en las instancias) en la Guía del usuario de Amazon VPC.
- El equipo local debe tener una dirección IPv6 y estar configurado para usar IPv6.

Error: no se puede cargar la clave... Se espera: CUALQUIER CLAVE PRIVADA

Si intenta conectarse a su instancia y obtiene el mensaje de error, `unable to load key ... Expecting: ANY PRIVATE KEY`, el archivo en el que está almacenada la clave privada está configurado de forma incorrecta. Si el archivo de clave privada termina en `.pem`, es posible que siga estando configurado de forma incorrecta. Una causa posible para un archivo de clave privada configurado incorrectamente es que falte un certificado.

Si el archivo de clave privada está configurado de forma incorrecta, siga estos pasos para resolver el error

1. Cree un nuevo par de claves. Para obtener más información, consulte Crear un par de claves mediante Amazon EC2.

   > **Note**
   >
   > Otra opción es crear un nuevo par de claves mediante una herramienta de terceros. Para obtener más información, consulte Crear un par de claves con una herramienta de terceros e importar la clave pública a Amazon EC2.

2. Añade el nuevo par de claves a su instancia. Para obtener más información, consulte Perdí mi clave privada. ¿Cómo puedo conectarme a mi instancia de Linux?.
3. Conecte a la instancia mediante el nuevo par de claves

Error: User key not recognized by server

Si usa SSH para conectarse con la instancia

- Use `ssh -vvv` para obtener información detallada de depuración triple:

```
ssh -vvv -i path/key-pair-name.pem instance-user-
name@ec2-203-0-113-25.compute-1.amazonaws.com
```

El resultado del ejemplo siguiente muestra lo que puede ver si intenta conectar con la instancia mediante una clave que el servidor no reconoce:

```
open/ANT/myusername/.ssh/known_hosts).
debug2: bits set: 504/1024
debug1: ssh_rsa_verify: signature correct
debug2: kex_derive_keys
debug2: set_newkeys: mode 1
debug1: SSH2_MSG_NEWKEYS sent
debug1: expecting SSH2_MSG_NEWKEYS
debug2: set_newkeys: mode 0
debug1: SSH2_MSG_NEWKEYS received
debug1: Roaming not allowed by server
debug1: SSH2_MSG_SERVICE_REQUEST sent
```

```
debug2: service_accept: ssh-userauth
debug1: SSH2_MSG_SERVICE_ACCEPT received
debug2: key: boguspem.pem ((nil))
debug1: Authentications that can continue: publickey
debug3: start over, passed a different list publickey
debug3: preferred gssapi-keyex,gssapi-with-mic,publickey,keyboard-
interactive,password
debug3: authmethod_lookup publickey
debug3: remaining preferred: keyboard-interactive,password
debug3: authmethod_is_enabled publickey
debug1: Next authentication method: publickey
debug1: Trying private key: boguspem.pem
debug1: read PEM private key done: type RSA
debug3: sign_and_send_pubkey: RSA 9c:4c:bc:0c:d0:5c:c7:92:6c:8e:9b:16:e4:43:d8:b2
debug2: we sent a publickey packet, wait for reply
debug1: Authentications that can continue: publickey
debug2: we did not send a packet, disable method
debug1: No more authentication methods to try.
Permission denied (publickey).
```

Si usa PuTTY para conectarse con la instancia

- Verifique que el archivo de clave privada (.pem) se ha convertido en el formato que reconoce PuTTY (.ppk). Para obtener más información acerca de la conversión de claves privadas, consulte Conéctese a la instancia de Linux desde Windows con PuTTY.

  > **Note**
  >
  > En PuTTYgen, cargue el archivo de clave privada y seleccione Guardar clave privada en lugar de Generar.

- Verifique que está conectando con el nombre de usuario adecuado para la AMI. Escriba el nombre de usuario en el cuadro Nombre de host de la ventana Configuración de PuTTY.

AMI utilizada para lanzar la instancia	Nombre de usuario predeterminado
AL2023 Amazon Linux 2	`ec2-user`

AMI utilizada para lanzar la instancia	Nombre de usuario predeterminado
Amazon Linux	
CentOS	`centos` o `ec2-user`
Debian	`admin`
Fedora	`fedora` o `ec2-user`
RHEL	`ec2-user` o `root`
SUSE	`ec2-user` o `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`
Rocky Linux	`rocky`
Otro	Comprobación con el proveedor de AMI

- Verifique que tiene una regla en el grupo de seguridad de entrada para permitir el tráfico de entrada en el puerto adecuado. Para obtener más información, consulte Reglas para conectarse a las instancias desde un equipo.

Error: Permiso denegado o conexión cerrada por [instancia] puerto 22

Si se conecta a la instancia mediante SSH y recibe alguno de los errores `Host key not found in [directory]`, `Permission denied (publickey)`, `Authentication failed, permission denied` o `Connection closed by [instance] port 22`, verifique que se está conectando con el nombre de usuario adecuado para la AMI y que ha especificado el archivo de clave privada adecuado (`.pem`) para la instancia.

Los nombres de usuario correctos son como siguen:

AMI utilizada para lanzar la instancia	Nombre de usuario predeterminado
AL2023 Amazon Linux 2 Amazon Linux	`ec2-user`
CentOS	`centos` o `ec2-user`
Debian	`admin`
Fedora	`fedora` o `ec2-user`
RHEL	`ec2-user` o `root`
SUSE	`ec2-user` o `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`
Rocky Linux	`rocky`
Otro	Comprobación con el proveedor de AMI

Por ejemplo, para utilizar un cliente SSH para conectarse a una instancia de Amazon Linux, utilice el siguiente comando:

```
ssh -i /path/key-pair-name.pem instance-user-
name@ec2-203-0-113-25.compute-1.amazonaws.com
```

Confirme que está usando el archivo de clave privada que corresponde al par de claves que ha seleccionado cuando lanzó la instancia.

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instances (Instancias) y, luego, seleccione la instancia.

3. En la ficha Details (Detalles), debajo de Instance details (Detalles de la instancia), compruebe el valor del Nombre del par de claves.
4. Si no ha especificado un par de claves cuando lanzó la instancia, puede terminarla y lanzar otra nueva, asegurando que especifica un par de claves. Si se trata de una instancia que ha estado usando pero que ya no tiene el archivo `.pem` para el par de claves, puede remplazarlo por uno nuevo. Para obtener más información, consulte Perdí mi clave privada. ¿Cómo puedo conectarme a mi instancia de Linux?.

Si generó un par de claves propias, asegúrese de que el generador de claves está configurado para crear claves RSA. Las claves DSA no se aceptan.

Si obtiene un error `Permission denied (publickey)` y nada de lo anterior se cumple (por ejemplo, previamente pudo conectarse), es posible que los permisos del directorio principal de la instancia hayan cambiado. Los permisos de `/home/`*`instance-user-name`*`/.ssh/authorized_keys` deben limitarse al propietario únicamente.

Para verificar los permisos de la instancia

1. Detenga la instancia y sepárela del volumen raíz. Para obtener más información, consulte Detención e iniciación de una instancia de Amazon EC2.
2. Lance una instancia temporal en la misma zona de disponibilidad que la instancia actual (use la misma AMI o una similar a la que usó para la instancia actual) y adjunte el volumen raíz a la instancia temporal.
3. Conéctese a la instancia temporal, cree un punto de montaje y monte el volumen que ha adjuntado.
4. Para la instancia temporal, compruebe los permisos del directorio `/home/`*`instance-user-name`*`/` del volumen adjunto. Si es necesario, ajuste los permisos como sigue:

```
[ec2-user ~]$ chmod 600 mount_point/home/instance-user-name/.ssh/authorized_keys
```

```
[ec2-user ~]$ chmod 700 mount_point/home/instance-user-name/.ssh
```

```
[ec2-user ~]$ chmod 700 mount_point/home/instance-user-name
```

5. Desmonte el volumen, sepárelo de la instancia temporal y vuelva a adjuntarlo a la instancia original. Asegúrese de que especifica el nombre de dispositivo correcto para el volumen raíz, por ejemplo, `/dev/xvda`.
6. Inicie la instancia. Si ya no necesita la instancia temporal, puede terminarla.

Error: Unprotected Private Key File (Error: archivo de clave privada no protegido)

El archivo de clave privada debe estar protegido frente a operaciones de lectura y escritura de otros usuarios. Si otra persona además de usted puede leer o escribir la clave privada, entonces SSH omite la clave y verá el siguiente mensaje de advertencia.

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0777 for '.ssh/my_private_key.pem' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
bad permissions: ignore key: .ssh/my_private_key.pem
Permission denied (publickey).
```

Si ve un mensaje similar cuando intenta iniciar sesión en la instancia, examine la primera línea del mensaje de error para verificar que está usando la clave pública correcta para la instancia. En el ejemplo anterior se usa la clave privada `.ssh/my_private_key.pem` con los permisos de archivo `0777`, que permite a cualquiera leer o escribir en este archivo. Este nivel de permiso es muy inseguro, de forma que SSH omite esta clave.

Si se conecta desde macOS o Linux, ejecute el siguiente comando para corregir el error y sustituya la ruta del archivo de clave privada.

```
[ec2-user ~]$ chmod 0400 .ssh/my_private_key.pem
```

Si se conecta desde Windows, siga estos pasos en su computadora local.

1. Vaya hasta el archivo .pem.
2. Haga clic con el botón derecho en el archivo .pem y seleccione Properties (Propiedades).
3. Elija la pestaña Seguridad.
4. Seleccione Advanced (Avanzado).

5. Compruebe que es el propietario del archivo. Si no es así, cambie el propietario a su nombre de usuario.
6. Seleccione Disable inheritance (Desactivar la herencia) y Remove all inherited permissions from this object (Eliminar todos los permisos heredados de este objeto).
7. Seleccione Add (Agregar), seleccione una entidad principal, ingrese su nombre de usuario y seleccione OK (Aceptar).
8. Desde la ventana Permission Entry (Entrada de permisos), conceda permisos de lectura y seleccione OK (Aceptar).
9. Haga clic en Apply (Aplicar) para asegurarse de que se guarde toda la configuración.
10. Seleccione OK (Aceptar) para cerrar la ventana Advanced Security Settings (Configuración de seguridad avanzada).
11. Seleccione OK (Aceptar) para cerrar la ventana Properties (Propiedades).
12. Debería poder conectarse a la instancia de Linux desde Windows a través de SSH.

En el símbolo del sistema de Windows, ejecute los siguientes comandos.

1. En el símbolo del sistema, vayas hasta la ubicación de ruta de acceso del archivo .pem.
2. Ejecute el siguiente comando para restablecer y eliminar los permisos explícitos:

```
icacls.exe $path /reset
```

3. Ejecute el siguiente comando para conceder permisos de lectura al usuario actual:

```
icacls.exe $path /GRANT:R "$($env:USERNAME):(R)"
```

4. Ejecute el siguiente comando para desactivar la herencia y eliminar los permisos heredados.

```
icacls.exe $path /inheritance:r
```

5. Debería poder conectarse a la instancia de Linux desde Windows a través de SSH.

Error: La clave privada debe empezar por "-----BEGIN RSA PRIVATE KEY-----" y terminar por "-----END RSA PRIVATE KEY-----"

Si utiliza una herramienta externa, como ssh-keygen, para crear un par de claves de RSA, la clave privada se genera con el formato de clave OpenSSH. Cuando se conecte a la instancia, si utiliza la

clave privada con el formato OpenSSH para descifrar la contraseña, aparecerá el error `Private key must begin with "-----BEGIN RSA PRIVATE KEY-----" and end with "-----END RSA PRIVATE KEY-----"`.

Para resolver el error, la clave privada debe tener el formato PEM. Utilice el siguiente comando para crear la clave privada con el formato PEM:

```
ssh-keygen -m PEM
```

Error: Server refused our key o No supported authentication methods available

Si usa PuTTY para conectar con la instancia y obtiene alguno de los errores siguientes, Error: el servidor rechazó nuestra clave o Error: no hay disponibles métodos de autenticación admitidos, verifique que se está conectando con el nombre de usuario adecuado para la AMI. Escriba el nombre de usuario en el cuadro Nombre de usuario de la ventana Configuración de PuTTY.

Los nombres de usuario correctos son como siguen:

AMI utilizada para lanzar la instancia	Nombre de usuario predeterminado
AL2023 Amazon Linux 2 Amazon Linux	`ec2-user`
CentOS	`centos` o `ec2-user`
Debian	`admin`
Fedora	`fedora` o `ec2-user`
RHEL	`ec2-user` o `root`
SUSE	`ec2-user` o `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`

AMI utilizada para lanzar la instancia	Nombre de usuario predeterminado
Bitnami	`bitnami`
Rocky Linux	`rocky`
Otro	Comprobación con el proveedor de AMI

También debe comprobar que:

- Está utilizando la última versión de PuTTY. Para obtener más información, consulte la Página web de PuTTY.
- Verifique que el archivo de clave privada (.pem) se ha convertido en el formato que reconoce PuTTY (.ppk). Para obtener más información acerca de la conversión de claves privadas, consulte Conéctese a la instancia de Linux desde Windows con PuTTY.

Cannot Ping Instance (No se puede ejecutar Ping en la instancia)

El comando `ping` es un tipo de tráfico ICMP — si no logra enviar un comando ping a la instancia, asegúrese de que las reglas de entrada del grupo de seguridad permiten el tráfico ICMP para el mensaje `Echo Request` desde todos los orígenes, o desde el equipo o la instancia desde la que ejecuta el comando.

Si no logra enviar un comando `ping` desde la instancia, asegúrese de que las reglas de salida del grupo de seguridad permiten el tráfico ICMP para el mensaje `Echo Request` a todos los destinos, o al host al que intenta mandar el comando.

Los comandos `Ping` también los puede bloquear un firewall o el tiempo de espera debido a problemas de latencia de red o hardware. Debe consultar a su administrador del sistema o red local para obtener ayuda para solución de problemas.

Error: el servidor ha cerrado inesperadamente la conexión de red

Si está conectando la instancia con PuTTY y recibe el error "El servidor ha cerrado inesperadamente la conexión de red", verifique que ha habilitado parámetros keepalives en la página Conexión de la Configuración de PuTTY para evitar la desconexión. Algunos servidores desconectan clientes cuando no reciben ningún dato dentro de un período de tiempo especificado. Defina el valor de segundos entre keepalives en 59 segundos.

Si sigue experimentando problemas después de habilitar los keepalives, pruebe a deshabilitar el algoritmo de Nagle en la página Conexión de la Configuración de PuTTY.

Error: no se pudo validar la clave de host para EC2 Instance Connect

Si rota las claves de host de instancia, las nuevas claves de host no se cargan de forma automática en la base de datos de claves de host de confianza de AWS. Esto provoca un error en la validación de la clave de host cuando intenta conectarse a la instancia mediante el cliente EC2 Instance Connect basado en explorador y no puede conectarse a la instancia.

Para resolver el error, debe ejecutar el script `eic_harvest_hostkeys` en la instancia, que carga la nueva clave de host en EC2 Instance Connect. El script se encuentra en `/opt/aws/bin/` en las instancias Amazon Linux 2 y en `/usr/share/ec2-instance-connect/` en las instancias de Ubuntu.

Amazon Linux 2

Para resolver el error de validación de la clave de host en una instancia Amazon Linux 2, haga lo siguiente:

1. Conéctese a la instancia mediante SSH.

   Puede conectarse mediante la interfaz de línea de comandos (CLI) EC2 Instance Connect o con el par de claves SSH que se asignó a su instancia cuando la lanzó y el nombre de usuario predeterminado de la AMI que utilizó para lanzar la instancia. Para Amazon Linux 2, el nombre de usuario predeterminado es `ec2-user`.

   Por ejemplo, si su instancia se lanzó usando Amazon Linux 2, el DNS público de la instancia es `ec2-a-b-c-d.us-west-2.compute.amazonaws.com` y el par de claves es `my_ec2_private_key.pem`. Use el siguiente comando para SSH en su instancia:

   ```
   $ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

   Para obtener más información sobre cómo conectarse a la instancia, consulte Conéctese a la instancia de Linux desde Linux o macOS mediante SSH..
2. Desplácese a la siguiente carpeta.

   ```
   [ec2-user ~]$ cd /opt/aws/bin/
   ```

3. Ejecute el siguiente comando en la instancia.

```
[ec2-user ~]$ ./eic_harvest_hostkeys
```

Tenga en cuenta que una llamada exitosa no da como resultado ninguna salida.

Ahora puede utilizar el cliente EC2 Instance Connect basado en explorador para conectarse a la instancia.

Ubuntu

Para resolver el error de validación de clave de host en una instancia de Ubuntu, haga lo siguiente:

1. Conéctese a la instancia mediante SSH.

Puede conectarse mediante la interfaz de línea de comandos (CLI) EC2 Instance Connect o con el par de claves SSH que se asignó a su instancia cuando la lanzó y el nombre de usuario predeterminado de la AMI que utilizó para lanzar la instancia. Para Ubuntu, el nombre de usuario predeterminado es `ubuntu`.

Por ejemplo, si su instancia se lanzó con Ubuntu, el nombre de DNS público de la instancia es `ec2-a-b-c-d.us-west-2.compute.amazonaws.com` y el par de claves es `my_ec2_private_key.pem`. Use el siguiente comando para SSH en la instancia:

```
$ ssh -i my_ec2_private_key.pem ubuntu@ec2-a-b-c-d.us-
west-2.compute.amazonaws.com
```

Para obtener más información sobre cómo conectarse a la instancia, consulte Conéctese a la instancia de Linux desde Linux o macOS mediante SSH..

2. Desplácese a la siguiente carpeta.

```
[ec2-user ~]$ cd /usr/share/ec2-instance-connect/
```

3. Ejecute el siguiente comando en la instancia.

```
[ec2-user ~]$ ./eic_harvest_hostkeys
```

Tenga en cuenta que una llamada exitosa no da como resultado ninguna salida.

Ahora puede utilizar el cliente EC2 Instance Connect basado en explorador para conectarse a la instancia.

No es posible conectarse a la instancia Ubuntu mediante EC2 Instance Connect

Si aparece un error al intentar conectarse a su instancia de Ubuntu mediante EC2 Instance Connect, puede utilizar la siguiente información para intentar solucionar el problema.

Causa posible

El paquete `ec2-instance-connect` de la instancia no es la última versión.

Solución

Actualice el paquete `ec2-instance-connect` de la instancia a la última versión, de la siguiente manera:

1. Conéctese a la instancia mediante un método que no sea EC2 Instance Connect.
2. Ejecute el siguiente comando en la instancia para actualizar el paquete `ec2-instance-connect` a la versión más reciente.

```
apt update && apt upgrade
```

Perdí mi clave privada. ¿Cómo puedo conectarme a mi instancia de Linux?

Si pierde la clave privada para una instancia respaldada por EBS, puede volver a obtener acceso a la instancia. Para ello, debe detener la instancia, desconectar su volumen raíz y asociarlo a otra instancia como volumen de datos, modificar el archivo `authorized_keys` con una nueva clave pública, trasladar el volumen de nuevo a la instancia original y reiniciar la instancia. Para obtener más información acerca de cómo lanzar, conectar y detener instancias, consulte Ciclo de vida de la instancia.

Este procedimiento solo se admite para instancias con volúmenes raíz de EBS. Si el dispositivo raíz es un volumen del almacén de instancias, no puede utilizar este procedimiento para recuperar el

acceso a la instancia; debe tener la clave privada para conectarse a la instancia. Para determinar el tipo de dispositivo raíz de la instancia, abra la consola de Amazon EC2, elija Instancias, seleccione la instancia, elija la pestaña Almacenamiento y, en la sección Detalles del dispositivo raíz compruebe el valor de Tipo de dispositivo raíz.

El valor es `EBS` o `INSTANCE-STORE`.

Además de los siguientes pasos, hay otras formas de conectarse a la instancia de Linux si extravía la clave privada. Para obtener más información, consulte ¿Cómo puedo conectarme a mi instancia de Amazon EC2 si he extraviado mi par de claves SSH después del lanzamiento inicial?

Pasos para conectarse a una instancia respaldada por EBS con un par de claves diferente

- Paso 1: Crear un nuevo par de claves
- Paso 2: Obtener información sobre la instancia original y su volumen raíz
- Paso 3: Detener la instancia original
- Paso 4: Lanzar una instancia temporal
- Paso 5: Desconectar el volumen raíz de la instancia original y asociarlo a la instancia temporal
- Paso 6: Agregar la nueva clave pública a authorized_keys en el volumen original montado en la instancia temporal
- Paso 7: Desmontar y desconectar el volumen original de la instancia temporal y volver a asociarlo a la instancia original
- Paso 8: Conectarse a la instancia original utilizando el nuevo par de claves
- Paso 9: Limpieza

Paso 1: Crear un nuevo par de claves

Cree un nuevo par de claves mediante la consola de Amazon EC2 o una herramienta de terceros. Si desea dar al nuevo par de claves el mismo nombre que tenía la clave privada que perdió, primero debe eliminar el par de claves existente. Para obtener información sobre cómo crear un par de claves, consulte Crear un par de claves mediante Amazon EC2 o Crear un par de claves con una herramienta de terceros e importar la clave pública a Amazon EC2.

Paso 2: Obtener información sobre la instancia original y su volumen raíz

Tome nota de la siguiente información porque la necesitará para completar este procedimiento.

Para obtener información sobre la instancia original

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. Elija Instances (Instancias) en el panel de navegación y, a continuación, seleccione la instancia a la que desee conectarse. (Nos referiremos a ella como la instancia original).
3. En la pestaña Details (Detalles), tome nota del ID de la instancia y del ID de la AMI.
4. En la pestaña Networking (Redes), tome nota de la zona de disponibilidad.
5. En la pestaña Storage (Almacenamiento), en Root device name (Nombre del dispositivo raíz), tome nota del nombre del dispositivo para el volumen raíz (por ejemplo, `/dev/xvda`). A continuación, en Block devices (Dispositivos de bloqueo), busque el nombre de este dispositivo y tome nota del ID del volumen (por ejemplo, vol-0a1234b5678c910de).

Paso 3: Detener la instancia original

Elija Instance state (Estado de la instancia) y Stop instance (Detener instancia). Si esta opción está desactivada, la instancia ya está detenida o bien su dispositivo raíz es un volumen de almacén de instancias.

> **Warning**
>
> Cuando detiene una instancia, se borran los datos contenidos en todos los volúmenes de almacén de instancias. Para conservar los datos de los volúmenes del almacén de instancias, asegúrese de realizar una copia de seguridad de ellos en un almacenamiento persistente.

Paso 4: Lanzar una instancia temporal

New console

Para iniciar una instancia temporal

1. En el panel de navegación, elija Instances (Instancias) y, a continuación, Launch Instances (Lanzar instancias).
2. En la sección Name and tags (Nobre y etiquetas), para Name (Nombre), ingrese Temporary (Provisorio).

3. En la sección Application and OS Images (Imágenes de aplicaciones y SO), seleccione la misma AMI que utilizó para lanzar la instancia original. Si esta AMI no está disponible, puede crear una AMI que puede utilizar a partir de la instancia detenida. Para obtener más información, consulte Creación de una AMI basada en Amazon EBS.
4. En la sección Instance type (Tipo de instancia), mantenga el tipo de instancia predeterminado.
5. En la sección Key pair (Par de claves), para Key pair name (Nombre del par de claves), seleccione el par de claves existente para utilizar o crear uno nuevo.
6. En la sección Network settings (Configuración de red), elija Edit (Editar) y, a continuación, para Subnet (Subred), seleccione una subred en la misma zona de disponibilidad que la instancia original.
7. En el panel Summary (Resumen), elija Launch (Lanzar).

Old console

Elija Launch Instances (Lanzar instancias) y, a continuación, utilice el launch wizard para lanzar una instancia temporal con las siguientes opciones:

- En la página Choose an AMI (Elegir una AMI), seleccione la misma AMI que utilizó para lanzar la instancia original. Si esta AMI no está disponible, puede crear una AMI que puede utilizar a partir de la instancia detenida. Para obtener más información, consulte Creación de una AMI basada en Amazon EBS.
- En la página Choose an Instance Type (Elegir un tipo de instancia), deje el tipo de instancia predeterminado que el asistente haya seleccionado.
- En la página Configure Instance Details (Configurar detalles de instancia), especifique la misma zona de disponibilidad que la de la instancia original. Si va a lanzar una instancia en una VPC, seleccione una subred en esta zona de disponibilidad.
- En la página Add Tags (Añadir etiquetas), añada la etiqueta `Name=Temporary` a la instancia para indicar que se trata de una instancia temporal.
- En la página Review (Revisión), seleccione Launch (Lanzar). Elija el par de claves que creó en el paso 1 y, a continuación, elija Launch Instances (Lanzar instancias).

Paso 5: Desconectar el volumen raíz de la instancia original y asociarlo a la instancia temporal

1. En el panel de navegación, elija Volumes (Volúmenes) y seleccione el volumen de dispositivo raíz para la instancia original (tomó nota del ID de su volumen en uno paso previo). Elija Actions (Acciones), Detach volume (Desconectar volumen) y, luego, Detach (Desconectar). Espere a que el estado del volumen cambie a `available`. (Es posible que necesite seleccionar el icono Actualizar).
2. Con el volumen todavía seleccionado, elija Actions (Acciones) y, a continuación, elija Attach Volume (Adjuntar volumen). Seleccione el ID de la instancia temporal, tome nota del nombre del dispositivo especificado en Device name (Nombre del dispositivo) (por ejemplo, `/dev/sdf`) y, a continuación, elija Attach volume (Adjuntar volumen).

> **Note**
>
> Si lanzó la instancia original a partir de una AMI de AWS Marketplace y el volumen contiene códigos de AWS Marketplace, primero debe detener la instancia temporal antes de poder adjuntar el volumen.

Paso 6: Agregar la nueva clave pública a **`authorized_keys`** en el volumen original montado en la instancia temporal

1. Conéctese a la instancia temporal.
2. Desde la instancia temporal, monte el volumen que adjuntó a la instancia para que pueda obtener acceso a su sistema de archivos. Por ejemplo, si el nombre de dispositivo es `/dev/sdf`, utilice los siguientes comandos para montar el volumen como `/mnt/tempvol`.

> **Note**
>
> El nombre de dispositivo podría aparecer de forma diferente en la instancia. Por ejemplo, los dispositivos montados como `/dev/sdf` podrían mostrarse como `/dev/xvdf` en la instancia. Algunas versiones de Red Hat (o sus variantes como CentOS), incluso pueden aumentar la letra final en cuatro caracteres, donde `/dev/sd`*`f`* se convierte en `/dev/xvd`*`k`*.

a. Utilice el comando lsblk para determinar si el volumen está particionado.

```
[ec2-user ~]$ lsblk
NAME    MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda    202:0    0    8G  0 disk
##xvda1 202:1    0    8G  0 part /
xvdf    202:80   0  101G  0 disk
##xvdf1 202:81   0  101G  0 part
xvdg    202:96   0   30G  0 disk
```

En el ejemplo anterior, `/dev/xvda` y `/dev/xvdf` son volúmenes particionados, mientras que `/dev/xvdg` no lo es. Si el volumen está particionado, monte la partición (`/dev/xvdf1`) en lugar del dispositivo tal cual (`/dev/xvdf`) en los siguientes pasos.

b. Cree un directorio temporal para montar el volumen.

```
[ec2-user ~]$ sudo mkdir /mnt/tempvol
```

c. Monte el volumen (o la partición) en el punto de montaje temporal utilizando el nombre del volumen o el nombre de dispositivo que identificó anteriormente. El comando requerido depende del sistema de archivos de su sistema operativo. Tenga en cuenta que el nombre de dispositivo puede aparecer de forma diferente en la instancia. Consulte note en el paso 6 para más información.

- Amazon Linux, Ubuntu y Debian

```
[ec2-user ~]$ sudo mount /dev/xvdf1 /mnt/tempvol
```

- Amazon Linux 2, CentOS, SUSE Linux 12 y RHEL 7.x

```
[ec2-user ~]$ sudo mount -o nouuid /dev/xvdf1 /mnt/tempvol
```

> **Note**
>
> Si recibe un error que indica que el sistema de archivos está corrupto, ejecute el comando siguiente para usar la utilidad fsck para comprobar el sistema de archivos y reparar cualquier problema:

```
[ec2-user ~]$ sudo fsck /dev/xvdf1
```

3. Desde la instancia temporal, utilice el siguiente comando para actualizar `authorized_keys` en el volumen montado con la nueva clave pública de `authorized_keys` para la instancia temporal.

> **Important**
>
> Los ejemplos siguientes utilizan el nombre de usuario de Amazon Linux `ec2-user`. Es posible que necesite sustituirlo por un nombre de usuario diferente, como `ubuntu` para las instancias de Ubuntu.

```
[ec2-user ~]$ cp .ssh/authorized_keys /mnt/tempvol/home/ec2-user/.ssh/
authorized_keys
```

Si esta copia funciona correctamente, puede proceder al paso siguiente.

(Opcional) De lo contrario, si no tiene permiso para editar archivos en `/mnt/tempvol`, debe actualizar el archivo mediante el comando sudo y, a continuación, comprobar los permisos del archivo para asegurarse de que podrá iniciar sesión en la instancia original. Use el siguiente comando para comprobar los permisos del archivo.

```
[ec2-user ~]$ sudo ls -l /mnt/tempvol/home/ec2-user/.ssh
total 4
-rw------- 1 222 500 398 Sep 13 22:54 authorized_keys
```

En el resultado de este ejemplo, *222* es el ID de usuario y *500* es el ID de grupo. A continuación, utilice el comando sudo para volver a ejecutar el comando de copia que produjo un error.

```
[ec2-user ~]$ sudo cp .ssh/authorized_keys /mnt/tempvol/home/ec2-user/.ssh/
authorized_keys
```

Ejecute el siguiente comando de nuevo para determinar si los permisos han cambiado.

```
[ec2-user ~]$ sudo ls -l /mnt/tempvol/home/ec2-user/.ssh
```

Si el ID de usuario y el ID de grupo han cambiado, use el siguiente comando para restaurarlos.

```
[ec2-user ~]$ sudo chown 222:500 /mnt/tempvol/home/ec2-user/.ssh/authorized_keys
```

Paso 7: Desmontar y desconectar el volumen original de la instancia temporal y volver a asociarlo a la instancia original

1. Desde la instancia temporal, desmonte el volumen que adjuntó para que pueda volver a adjuntarlo a la instancia original. Por ejemplo, utilice el siguiente comando para desmontar el volumen en `/mnt/tempvol`.

   ```
   [ec2-user ~]$ sudo umount /mnt/tempvol
   ```

2. Desconecte el volumen de la instancia temporal (lo desmontó en el paso anterior): en la consola de Amazon EC2 elija Volumes (Volúmenes) en el panel de navegación, seleccione el volumen del dispositivo raíz de la instancia original (tomó nota del ID del volumen en un paso anterior), elija Actions (Acciones), Detach volume (Desconectar volumen) y, luego, Detach (Desconectar). Espere a que el estado del volumen cambie a `available`. (Es posible que necesite seleccionar el icono Refresh (Actualizar)).
3. Vuelva a conectar el volumen a la instancia original: con el volumen seleccionado, elija Actions (Acciones), Attach Volume (Adjuntar volumen). Seleccione el ID de la instancia original, especifique el nombre de dispositivo que anotó anteriormente en el paso 2 para el adjunto del dispositivo raíz original (`/dev/sda1` o `/dev/xvda`) y, a continuación, elija Attach volume (Adjuntar volumen).

   > **Important**
   >
   > Si no especifica el mismo nombre de dispositivo que el de la asociación original, no podrá comenzar la instancia original. Amazon EC2 espera que el volumen de dispositivo raíz sea `sda1` o `/dev/xvda`.

Paso 8: Conectarse a la instancia original utilizando el nuevo par de claves

Seleccione la instancia original y elija Instance state (Estado de la instancia) y Start instance (Iniciar instancia). Cuando la instancia pase a estado `running`, puede conectarse a ella utilizando el archivo de clave privada para su nuevo par de claves.

> **Note**
>
> Si el nombre de su nuevo par de claves y del archivo de clave privada correspondiente es diferente al del par de claves original, asegúrese de especificar el nombre del nuevo archivo de clave privada al conectarse a la instancia.

Paso 9: Limpieza

(Opcional) Puede terminar la instancia temporal cuando no vaya a utilizarla más. Seleccione la instancia temporal y elija Instance state (Estado de la instancia) y Terminate instance (Terminar instancia).

Solucionar problemas con la conexión a la instancia de Windows

La información y los errores comunes que se presentan a continuación pueden ayudarlo a solucionar problemas relacionados con la conexión a la instancia de Windows.

Problemas de conectividad

- El escritorio remoto no puede conectarse al equipo remoto
- Error al usar el cliente RDP de macOS
- RDP muestra una pantalla negra en lugar del escritorio
- No se puede iniciar sesión de manera remota en una instancia con un usuario que no sea un administrador
- Solución de problemas escritorio remoto mediante AWS Systems Manager
- Habilitación del escritorio remoto en una instancia de EC2 con el registro remoto
- Perdí mi clave privada. ¿Cómo puedo conectarme a mi instancia de Windows?

El escritorio remoto no puede conectarse al equipo remoto

Pruebe lo siguiente para solucionar los problemas de conexión con la instancia:

- Verifique que está usando el nombre de host DNS público correcto. (En la consola de Amazon EC2, seleccione la instancia y compruebe Public DNS (IPv4) (DNS público (IPv4)) en el panel de detalles). Si la instancia está en una VPC y no ve un nombre DNS público, debe habilitar los nombres de host DNS. Para obtener más información, consulte Atributos de DNS para su VPC en la Guía del usuario de Amazon VPC.
- Verifique que la instancia tiene una dirección IPv4 pública. Si no, asocie una dirección IP elástica a su instancia. Para obtener más información, consulte Direcciones IP elásticas.
- Para conectar con la instancia usando una dirección IPv6 pública, compruebe que el equipo local tiene una dirección IPv6 y que está configurada para usar IPv6. Para obtener más información, consulte Configure IPv6 on your instances (Configuración de IPv6 en las instancias) en la Guía del usuario de Amazon VPC.
- Verifique que el grupo de seguridad tiene una regla que permite el acceso RDP.
- Si ha copiado la contraseña pero recibe el error `Your credentials did not work`, intente escribirla manualmente cuando se indique. Es posible que faltara un carácter o que hubiera un espacio en blanco extra cuando copió la contraseña.
- Verifique que la instancia ha pasado las comprobaciones de estado. Para obtener más información, consulte Comprobaciones de estado para sus instancias y the section called “Comprobaciones de estado no superadas en Linux”.
- Verifique que la tabla de ruteo de la subred tiene una ruta que envía todo el tráfico destinado fuera de la VPC al gateway de Internet de la VPC. Para obtener más información, consulta Crear una tabla de enrutamiento personalizada (Gateways de Internet) en la Guía del usuario de Amazon VPC.
- Verifique que Windows Firewall, u otro software de firewall, no está bloqueando el tráfico RDP a la instancia. Recomendamos que deshabilite Windows Firewall y controle el acceso a la instancia usando las reglas del grupo de seguridad. Puede utilizar AWSSupport-TroubleshootRDP para disable the Windows Firewall profiles using SSM Agent. Para deshabilitar el firewall de Windows en una instancia de Windows que no esté configurada para AWS Systems Manager, utilice AWSSupport-ExecuteEC2Rescue o siga los siguientes pasos manuales:

Procedimiento manual

1. Detenga la instancia afectada y sepárela del volumen raíz.
2. Lance una instancia temporal en la misma zona de disponibilidad que la instancia afectada.

> **Warning**
>
> Si la instancia temporal se basa en la misma AMI que la instancia original, debe completar otros pasos o no podrá arrancar la instancia original después de restaurar el volumen raíz debido a un conflicto de firmas de disco. Como alternativa, selecciones una AMI diferente para la instancia temporal. Por ejemplo, si la instancia original utiliza una AMI de Windows de AWS para Windows Server 2016, lance la instancia temporal mediante el uso de una AMI de Windows de AWS para Windows Server 2019.

3. Adjunte el volumen raíz de la instancia afectada a esta instancia temporal. Conéctese a la instancia temporal, abra la utilidad Administración de discos y ponga la unidad online.
4. Abra Regedit y seleccione HKEY_LOCAL_MACHINE. En el menú Archivo, elija Cargar Hive. Seleccione la unidad, abra el archivo `Windows\System32\config\SYSTEM` y especifique un nombre de clave cuando se solicite (puede usar cualquier nombre).
5. Seleccione la clave que acaba de cargar y navegue hasta `ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy`. Para cada clave cuyo nombre tenga el formato xxxxProfile, seleccione la clave y cambie `EnableFirewall` de 1 a 0. Seleccione la clave de nuevo y en el menú Archivo, elija Descargar Hive.
6. (Opcional) Si la instancia temporal se basa en la misma AMI que la instancia original, debe completar los siguientes pasos o no podrá arrancar la instancia original después de restaurar el volumen raíz debido a un conflicto de firmas de disco.

> **Warning**
>
> En el siguiente procedimiento se describe cómo editar el Registro de Windows mediante el Editor del Registro. Si no está familiarizado con el Registro de Windows o cómo realizar cambios de forma segura mediante el Editor del Registro, consulte Configuración del Registro.

   a. Abra un símbolo del sistema, escriba regedit.exe y, a continuación, presione Enter (Intro).
   b. En el navegador Registry Editor (Editor del Registro), elija HKEY_LOCAL_MACHINE desde el menú contextual (haga clic con el botón derecho) y, luego, elija Find (Buscar).
   c. Escriba Windows Boot Manager y, luego, elija Find Next (Buscar siguiente).

d. Elija la clave denominada `11000001`. Esta clave es un elemento secundario de la clave que encontró en el paso anterior.

e. En el panel derecho, elija `Element` y, a continuación, elija Modify (Modificar) desde el menú contextual (haga clic con el botón derecho).

f. Localice la firma del disco de cuatro bytes en el desplazamiento 0x38 en los datos. Invierta los bytes para crear la firma del disco y escríbalo. Por ejemplo, la firma de disco que se representa con los siguientes datos es `E9EB3AA5`:

```
...
0030  00 00 00 00 01 00 00 00
0038  A5 3A EB E9 00 00 00 00
0040  00 00 00 00 00 00 00 00
...
```

g. En una ventana del símbolo del sistema, ejecute el siguiente comando para iniciar Microsoft DiskPart.

```
diskpart
```

h. Ejecute el siguiente comando “DiskPart” para seleccionar el volumen. (Puede verificar que el número de disco es 1 mediante la utilidad Administración de discos).

```
DISKPART> select disk 1

Disk 1 is now the selected disk.
```

i. Ejecute el siguiente comando “DiskPart” para obtener la firma del disco.

```
DISKPART>  uniqueid disk

Disk ID: 0C764FA8
```

j. Si la firma de disco que se muestra en el paso anterior no coincide con la del disco de BCD que escribió anteriormente, utilice el siguiente comando “DiskPart” para cambiar la firma de disco de manera que coincida:

```
DISKPART> uniqueid disk id=E9EB3AA5
```

7. Use la utilidad Administración de discos para desconectar la unidad.

> **Note**
>
> La unidad queda automáticamente sin conexión si la instancia temporal ejecuta el mismo sistema operativo que la instancia afectada, por lo que no tendrá que desconectarla manualmente.

8. Separe el volumen de la instancia temporal. Puede terminar la instancia temporal si no va a utilizarla más.
9. Restaure el volumen raíz de la instancia afectada adjuntándolo como `/dev/sda1`.
10. Inicie la instancia.

- Compruebe que la autenticación de red está deshabilitada en las instancias que no formen parte de un dominio de Active Directory (use AWSSupport-TroubleshootRDP para disable NLA).
- Compruebe que el tipo de inicio del servicio de escritorio remoto (TermService) sea Automático y que el servicio esté iniciado (utilice AWSSupport-TroubleshootRDP para enable and start the RDP service).
- Compruebe que se efectúe la conexión al puerto correcto del protocolo de escritorio remoto, que es el 3389 de forma predeterminada (utilice AWSSupport-TroubleshootRDP para read the current RDP port y change it back to 3389).
- Compruebe que se permitan conexiones al escritorio remoto en la instancia (utilice AWSSupport-TroubleshootRDP para enable Remote Desktop connections).
- Verifique que la contraseña no ha caducado. Si la contraseña ha caducado, puede restablecerla. Para obtener más información, consulte Restablecer una contraseña de administrador de Windows perdida o vencida.
- Si intenta conectarse mediante un usuario que creó en la instancia y recibe el error `The user cannot connect to the server due to insufficient access privileges`, compruebe que le concedió permiso para iniciar sesión de manera local. Para obtener más información, consulte Concesión de un permiso para iniciar sesión de manera local a un miembro.
- Si intenta más sesiones RDP simultáneas del máximo permitido, la sesión termina con el mensaje `Your Remote Desktop Services session has ended. Another user connected to the remote computer, so your connection was lost.` De manera predeterminada, solo se permiten dos sesiones RDP simultáneas en la instancia.

Error al usar el cliente RDP de macOS

Si se conecta con una instancia de Windows Server mediante el cliente de Conexión de escritorio remoto en el sitio web de Microsoft, es posible que aparezca el siguiente error:

```
Remote Desktop Connection cannot verify the identity of the computer that you want to
 connect to.
```

Descargue la aplicación Escritorio remoto de Microsoft desde la Mac App Store y úsela para conectar con su instancia.

RDP muestra una pantalla negra en lugar del escritorio

Pruebe lo siguiente para resolver este problema:

- Consulte el resultado de la consola si desea información adicional. Para obtener la salida de la consola de la instancia utilizando la consola Amazon EC2, selecciona la instancia, luego selecciona Acciones, luego selecciona Supervisar y solucionar problemas y a continuación selecciona Obtener registro del sistema.
- Verifique que está ejecutando la última versión del cliente RDP.
- Pruebe la configuración predeterminada para el cliente RDP. Para obtener más información, consulte Remote Session Environment.
- Si usa Conexión de Escritorio Remoto, intente iniciarla con la opción `/admin` como sigue.

  ```
  mstsc /v:instance /admin
  ```

- Si el servidor ejecuta una aplicación a pantalla completa, es posible que haya dejado de responder. Use Ctrl+Shift+Esc para iniciar el Administrador de tareas de Windows y, después, cierre la aplicación.
- Si el servidor está siendo utilizado en exceso, es posible que haya dejado de responder. Para monitorizar la instancia usando la consola de Amazon EC2, seleccione la instancia y, a continuación, seleccione la pestaña Monitoring (Monitorización). Si necesita cambiar el tipo de instancia por una de mayor tamaño, consulte Cambie el tipo de instancia.

No se puede iniciar sesión de manera remota en una instancia con un usuario que no sea un administrador

Si no puede iniciar sesión de manera remota en una instancia de Windows con un usuario que no sea una cuenta de administrador, asegúrese de que le ha concedido permiso para iniciar sesión de manera local. Consulte Grant a user or group the right to log on locally to the domain controllers in the domain.

Solución de problemas escritorio remoto mediante AWS Systems Manager

Puede utilizar AWS Systems Manager para solucionar problemas de conexión a su instancia de Windows mediante RDP.

AWSSupport-TroubleshootRDP

El documento de automatización AWSSupport-TroubleshootRDP permite al usuario comprobar o modificar los ajustes comunes de la instancia de destino que pueden afectar a las conexiones del protocolo de escritorio remoto (RDP), tales como los perfiles de Puerto RDP, Autenticación en el nivel de red (NLA) y Firewall de Windows. De forma predeterminada, el documento lee los valores de estos ajustes y los incluye en la salida.

El documento de automatización AWSSupport-TroubleshootrDP se puede utilizar con instancias EC2, instancias locales y máquinas virtuales (VM) habilitadas para su uso con AWS Systems Manager (instancias administradas). Además, también se puede usar con instancias EC2 para Windows Server que no estén habilitadas para su uso con Systems Manager. Para obtener más información sobre la habilitación de instancias para su uso con AWS Systems Manager, consulte Managed nodes (Nodos administrados) en la Guía del usuario de AWS Systems Manager.

Para solucionar problemas con el documento AWSSupport-TroubleshootRDP

1. Iniciar sesión en la Consola de Systems Manager.
2. Compruebe que se encuentra en la misma región que la instancia deteriorada.
3. En el panel de navegación izquierdo, elija Documents (Documentos).
4. En la pestaña Owned by Amazon (Propiedad de Amazon), ingrese `AWSSupport-TroubleshootRDP` en el campo de búsqueda. Cuando aparezca el documento `AWSSupport-TroubleshootRDP`, selecciónelo.
5. Elija Ejecutar automatización.

6. En Execution Mode (Modo de ejecución), elija Simple execution (Ejecución sencilla).
7. En Input parameters (Parámetros de entrada), InstanceId, active Show interactive instance picker (Mostrar selector de instancias interactivo).
8. Seleccione la instancia Amazon EC2.
9. Revise los ejemplos y elija Execute (Ejecutar).
10. Para monitorear el progreso de la ejecución, observe Execution status (Estado de ejecución) y espere a que cambie de Pending (Pendiente) a Success (Correcta). Expanda Outputs (Resultados) para ver los resultados. Para ver la salida de los pasos individuales, en Executed Steps (Pasos ejecutados), elija un elemento en Step ID (ID de paso).

Ejemplos de AWSSupport-TroubleshootRDP

En los ejemplos siguientes se muestra cómo llevar a cabo tareas de solución de problemas habituales con AWSSupport-TroubleshootRDP. Puede utilizar el comando start-automation-execution de ejemplo de la AWS CLI o el enlace proporcionado en la AWS Management Console.

Example Ejemplo: Comprobar el estado de RDP actual

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP" --
parameters "InstanceId=instance_id, Action=Custom" --region region_code
```

Consola de AWS Systems Manager:

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region#documentVersion=$LATEST
```

Example Ejemplo: Deshabilitación del Firewall de Windows

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP"
 --parameters "InstanceId=instance_id, Action=Custom, Firewall=Disable" --
region region_code
```

Consola de AWS Systems Manager:

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region_code#documentVersion=$LATEST&Firewall=Disable
```

Example Ejemplo: Deshabilitación de autenticación a nivel de red

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP"
 --parameters "InstanceId=instance_id, Action=Custom, NLASettingAction=Disable" --
region region_code
```

Consola de AWS Systems Manager:

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region_code#documentVersion
```

Example Ejemplo: Establecimiento del tipo de inicio del servicio de RDP en automático e inicio del servicio RDP

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP"
 --parameters "InstanceId=instance_id, Action=Custom, RDPServiceStartupType=Auto,
 RDPServiceAction=Start" --region region_code
```

Consola de AWS Systems Manager:

```
https://console.aws.amazon.com/systems-manager/automation/execute/
AWSSupport-TroubleshootRDP?region=region_code#documentVersion=
$LATEST&RDPServiceStartupType=Auto&RDPServiceAction=Start
```

Example Ejemplo: Restauración del puerto de RDP predeterminado (3389)

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP"
 --parameters "InstanceId=instance_id, Action=Custom, RDPPortAction=Modify" --
region region_code
```

Consola de AWS Systems Manager:

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region_code#documentVersion=$LATEST&RDPPortAction=Modify
```

Example Ejemplo: Autorización de conexiones remotas

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP"
 --parameters "InstanceId=instance_id, Action=Custom, RemoteConnections=Enable" --
region region_code
```

Consola de AWS Systems Manager:

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region_code#documentVersion=$LATEST&RemoteConnections=Enable
```

AWSSupport-ExecuteEC2Rescue

El documento de automatización AWSSupport-ExecuteEC2Rescue utiliza EC2Rescue for Windows Server para realizar automáticamente las tareas de solución de problemas y restauración de la conectividad de la instancia EC2 y de RDP. Para obtener más información, consulte Ejecutar la herramienta EC2Rescue en instancias inaccesibles.

El documento de automatización AWSSupport-ExecuteEC2Rescue requiere detener y volver a iniciar la instancia. La automatización de Systems Manager detiene la instancia y crea una Amazon Machine Image (AMI). Los datos guardados en los volúmenes de almacén de instancias se pierden. La dirección IP pública cambia si no se utiliza una dirección IP elástica. Para obtener más información, consulte Ejecutar la herramienta EC2Rescue en instancias inaccesibles en la Guía del usuario de AWS Systems Manager.

Para solucionar problemas con el documento AWSSupport-ExecuteEC2Rescue

1. Abra la consola de Systems Manager.
2. Compruebe que se encuentra en la misma región que la instancia Amazon EC2 deteriorada.
3. En el panel de navegación, elija Documentos.
4. Busque y seleccione el documento `AWSSupport-ExecuteEC2Rescue` y, a continuación, elija Ejecutar automatización.

5. En Execution Mode (Modo de ejecución), elija Simple execution (Ejecución sencilla).
6. En la sección Input parameters (Parámetros de entrada), en UnreachableInstanceId, especifique el ID de instancia de Amazon EC2 de la instancia inaccesible.
7. (Opcional) En LogDestination, especifique el nombre del bucket de Amazon Simple Storage Service (Amazon S3) si desea recopilar los logs del sistema operativo para usarlos en la solución de problemas de la instancia de Amazon EC2. Los registros se cargan automáticamente en el bucket especificado.
8. Elija Execute (Ejecutar).
9. Para monitorizar el progreso de la ejecución, observe Execution status (Estado de ejecución) y espere a que cambie de Pending (Pendiente) a Success (Correcta). Expanda Outputs (Resultados) para ver los resultados. Para ver la salida de los pasos individuales, en Executed Steps (Pasos ejecutados), elija el Step ID (ID de paso).

Habilitación del escritorio remoto en una instancia de EC2 con el registro remoto

Si el administrador de sesiones de AWS Systems Manager no administra la instancia a la que no se puede obtener acceso, puede utilizar el Registro remoto para habilitar Escritorio remoto.

1. Desde la consola de EC2, detenga la instancia a la que no se puede tener acceso.
2. Desasocie el volumen raíz de la instancia que no es accesible y asócielo a otra instancia accesible en la misma zona de disponibilidad que el volumen de almacenamiento. Si no dispone de una instancia accesible en la misma zona de disponibilidad, lance una. Anote el nombre del dispositivo del volumen raíz de la instancia que no es accesible.
3. En la instancia con acceso, abra Administración de discos. Para ello, ejecute el siguiente comando en una ventana de símbolo del sistema.

   ```
   diskmgmt.msc
   ```

4. Haga clic con el botón derecho en el volumen recién asociado que proviene de la instancia que no es accesible y, a continuación, seleccione En línea.
5. Abra el Editor del Registro de Windows. Para ello, ejecute el siguiente comando en una ventana de símbolo del sistema.

   ```
   regedit
   ```

6. En el Editor del Registro, elija HKEY_LOCAL_MACHINE y, a continuación, seleccione Archivo, Cargar Hive.
7. Seleccione la unidad del volumen asociado, desplácese hasta `\Windows\System32\config\`, seleccione `SYSTEM` y, a continuación, elija Abrir.
8. En Nombre de clave, escriba un nombre único para el hive y elija Aceptar.
9. Realice una copia de seguridad del hive del Registro antes de realizar cambios en el Registro.
   a. En el Editor del Registro, seleccione el hive que haya cargado: HKEY_LOCAL_MACHINE*your-key-name*.
   b. Elija Archivo>Exportar.
   c. En el cuadro de diálogo Exportar archivo del Registro, elija la ubicación en la que desea guardar la copia de seguridad y, a continuación, escriba un nombre para el archivo de copia de seguridad en el campo Nombre de archivo.
   d. Seleccione Guardar.
10. En el Editor del Registro, vaya a `HKEY_LOCAL_MACHINE\`*`your key name`*`\ControlSet001\Control\Terminal Server` y, a continuación, en el panel de detalles, haga doble clic en fDenyTSConnections.
11. En el cuadro Editar valor DWORD escriba `0` en el campo Información del valor.
12. Seleccione OK.

> **Note**
>
> Si el valor del campo Información del valor es `1`, la instancia denegará las conexiones de Escritorio remoto. Un valor de `0` permite conexiones de Escritorio remoto.

13. En el Editor del Registro, elija HKEY_LOCAL_MACHINE*your-key-name* y, a continuación, seleccione Archivo, Descargar Hive.
14. Cierre el Editor del Registro y la Administración de discos.
15. Desde la consola de EC2, desasocie el volumen de la instancia accesible y, a continuación, vuelva a asociarlo a la instancia que no es accesible. Al asociar el volumen a la instancia que no es accesible, escriba el nombre el dispositivo que guardó anteriormente en el campo device.
16. Detenga la instancia sin acceso.

Perdí mi clave privada. ¿Cómo puedo conectarme a mi instancia de Windows?

Cuando se conecta a una instancia de Windows recién lanzada, la contraseña de la cuenta de administrador se descifra mediante la clave privada del par de claves que se especificó al lanzar la instancia.

Si pierde la contraseña del administrador y ya no tiene la clave privada, debe restablecer la contraseña o crear una nueva instancia. Para obtener más información, consulte Restablecer una contraseña de administrador de Windows perdida o vencida. Para ver los pasos para restablecer la contraseña mediante un documento de Systems Manager, consulte Restablecer contraseñas y claves de SSH en instancias EC2 en la Guía del usuario de AWS Systems Manager.

Restablecer una contraseña de administrador de Windows perdida o vencida

> **Note**
>
> Esta sección se aplica únicamente a las instancias de Windows.

Si ya no puede acceder a su instancia Amazon EC2 de Windows porque ha perdido o ha caducado la contraseña de administrador de Windows puede restablecer la contraseña.

> **Note**
>
> Existe un documento de automatización de AWS Systems Manager que aplica de manera automática los pasos manuales necesarios para restablecer la contraseña del administrador local. Para obtener más información, consulte Restablecimiento de contraseñas y claves de SSH en instancias de EC2 en la Guía del usuario de AWS Systems Manager.

Los métodos manuales para restablecer la contraseña de administrador utilizan EC2Launch v2, EC2Config o EC2Launch.

- Para todas las AMI de Windows compatibles que incluyen el agente EC2Launch v2, use EC2Launch v2.

- En el caso de las AMI de Windows anteriores a Windows Server 2016, utilice el servicio EC2Config.
- En cuanto a las AMI de Windows Server 2016 y versiones posteriores, utilice el servicio EC2Launch.

Asimismo, estos procedimientos describen el modo en que puede conectarse a una instancia si pierde el par de claves que utilizó para crearla. En Amazon EC2, se utiliza una clave pública para cifrar determinados datos, como, por ejemplo, una contraseña y una clave privada para descifrarlos. El conjunto de clave pública y clave privada se denomina par de claves. Con instancias de Windows, se usa un par de claves para obtener la contraseña de administrador y después iniciar sesión mediante RDP.

> **Note**
>
> Si ha deshabilitado la cuenta de administrador local en la instancia y esta está configurada para Systems Manager, también puede volver a habilitar y restablecer la contraseña de administrador local por medio de EC2Rescue y Run Command. Para obtener más información, consulte Uso de EC2Rescue para Windows Server con Systems Manager Run Command.

Contenido

Restablecer la contraseña de administrador de Windows mediante EC2Launch v2

Si perdió la contraseña de administrador de Windows y utiliza una AMI de Windows compatible que incluye el agente EC2Launch v2, puede utilizar EC2Launch v2 para generar una nueva contraseña.

Si utiliza una AMI de Windows Server 2016 o una versión posterior que no incluye el agente EC2Launch v2, consulte Restablecer la contraseña de administrador de Windows mediante EC2Launch.

Si utiliza una AMI de Windows Server anterior a Windows Server 2016 que no incluye el agente EC2Launch v2, consulte Restablecer la contraseña de administrador de Windows mediante EC2Config.

> **Note**
>
> Si ha deshabilitado la cuenta de administrador local en la instancia y esta está configurada para Systems Manager, también puede volver a habilitar y restablecer la contraseña de administrador local por medio de EC2Rescue y Run Command. Para obtener más información, consulte Uso de EC2Rescue para Windows Server con Systems Manager Run Command.

> **Note**
>
> Existe un documento de automatización de AWS Systems Manager que aplica de manera automática los pasos manuales necesarios para restablecer la contraseña del administrador local. Para obtener más información, consulte Restablecimiento de contraseñas y claves de SSH en instancias de EC2 en la Guía del usuario de AWS Systems Manager.

Para restablecer la contraseña de administrador de Windows mediante EC2Launch v2, tiene que hacer lo siguiente:

- Paso 1: Comprobar que el agente EC2Launch v2 está en ejecución
- Paso 2: Separar el volumen raíz de la instancia
- Paso 3: Adjuntar el volumen a una instancia temporal
- Paso 4: Eliminar el archivo .run-once
- Paso 5: Reiniciar la instancia original

Paso 1: Comprobar que el agente EC2Launch v2 está en ejecución

Antes de intentar restablecer la contraseña de administrador, compruebe que el agente EC2Launch v2 está instalado y en ejecución. Utilizará el agente EC2Launch v2 para restablecer la contraseña de administrador más adelante en esta sección.

Para comprobar que el agente EC2Launch v2 está en ejecución

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancias) y luego, la instancia que necesita restablecer la contraseña. Esta instancia se denomina instancia original en este procedimiento.
3. Elija Actions (Acciones), Monitor and troubleshoot (Monitoreo y solución de problemas), Get system log (Obtener registro del sistema).
4. Localice la entrada de lanzamiento de EC2, por ejemplo, Launch: EC2Launch v2 service v2.0.124 (Lanzar: servicio EC2Launch v2 v2.0.124). Si ve esta entrada, el servicio EC2Launch v2 está en ejecución.

   Si el resultado del registro del sistema está vacío o si el agente EC2Launch v2 no está en ejecución, solucione los problemas de la instancia con el servicio de capturas de pantalla de consola de instancias. Para obtener más información, consulte Captura de pantalla de una instancia inaccesible.

Paso 2: Separar el volumen raíz de la instancia

No puede utilizar EC2Launch v2 para restablecer una contraseña de administrador si el volumen donde se almacena la contraseña está asociado a una instancia como volumen raíz. Debe separar el volumen de la instancia original para que pueda adjuntarlo a una instancia temporal como volumen secundario.

Desconectar el volumen raíz de la instancia

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Seleccione la instancia que requiere el restablecimiento de la contraseña y elija Estado de instancia, Detener instancia. Después de que el estado de la instancia cambie a Stopped (Detenido), proceda con el siguiente paso.
4. (Opcional) Si dispone de la clave privada que especificó cuando lanzó esta instancia, proceda con el siguiente paso. De lo contrario, siga los pasos siguientes para reemplazar la instancia por una nueva que se lance con un nuevo par de claves.

   a. Cree un nuevo par de claves mediante la consola de Amazon EC2. Si desea dar al nuevo par de claves el mismo nombre que tenía la clave privada que perdió, primero debe eliminar el par de claves existente.

b. Seleccione la instancia que desea reemplazar. Tenga en cuenta el tipo de instancia, la VPC, la subred, el grupo de seguridad y el rol de IAM de la instancia.

c. Elija Actions (Acciones), Image and templates (Imagen y plantillas), Create image (Crear imagen). Escriba un nombre y una descripción para la imagen y, luego, elija Create image (Crear imagen). En el panel de navegación, elija AMIs. Una vez que el estado de la imagen cambie a available (disponible), proceda con el paso siguiente.

d. Seleccione la imagen y elija Actions (Acciones) y, a continuación, Launch (Lanzar).

e. Complete el asistente con el mismo tipo de instancia, VPC, subred, grupo de seguridad y rol de IAM que la instancia que se desea reemplazar y, a continuación, seleccione Launch (Lanzar).

f. Cuando se solicite, elija el par de claves que creó para la nueva instancia, seleccione la casilla de confirmación y, a continuación, elija Launch Instances (Lanzar instancias).

g. (Opcional) Si la instancia original tenía una dirección IP elástica asociada, transfiérala a la nueva instancia. Si la instancia original tiene volúmenes de EBS además del volumen raíz, transfiéralos a la nueva instancia.

5. Desconecte el volumen raíz de la instancia original de la siguiente manera:

   a. Seleccione la instancia original y elija la pestaña Almacenamiento. Anote el nombre del dispositivo raíz en Nombre del dispositivo raíz. Busque el volumen con el nombre de este dispositivo en Dispositivos de bloques y anote el ID del volumen.

   b. En el panel de navegación, elija Volumes (Volúmenes).

   c. En la lista de volúmenes, seleccione el volumen que anotó como dispositivo raíz y elija Acciones, Separar volumen. Una vez que el estado del volumen cambie a available (disponible), siga con el paso siguiente.

6. Si creó una instancia nueva para reemplazar la instancia original, puede terminar la original ahora. Ya no se necesita. Para el resto del procedimiento, todas las referencias a la instancia original se aplican a la que acaba de crear.

Paso 3: Adjuntar el volumen a una instancia temporal

A continuación, lance una instancia temporal y adjúntele el volumen como volumen secundario. Esta es la instancia que debe utilizar para modificar el archivo de configuración.

Para lanzar una instancia temporal y adjuntar el volumen

1. Lance la instancia temporal de la siguiente manera:

   a. En el panel de navegación, elija Instances (Instancias), luego elija Launch instances (Lanzar instancias) y por último, seleccione una AMI.

   > **Important**
   >
   > Es necesario seleccionar una AMI para una versión diferente de Windows a fin de impedir que se produzcan conflictos de firmas de disco. Por ejemplo, si la instancia original ejecuta Windows Server 2019, lance la instancia temporal mediante el uso de una AMI para Windows Server 2016.

   b. Mantenga el tipo de instancia predeterminada y, a continuación, seleccione Next: Configure Instance Details (Siguiente: Configurar detalles de la instancia).

   c. En la página Configure Instance Details (Configurar detalles de la instancia), para Subred, seleccione la misma zona de disponibilidad que la de la instancia original y elija Review and Launch (Revisar y lanzar).

   > **Important**
   >
   > La instancia temporal debe estar en la misma zona de disponibilidad que la instancia original. Si su instancia temporal se encuentra en una zona de disponibilidad diferente, no podrá adjuntar a ella el volumen raíz de la instancia original.

   d. En la página Review Instance Launch, elija Launch.

   e. Cuando lo solicite, cree un nuevo par de claves, descárguelas en un lugar seguro de su computadora y, a continuación, elija Launch Instances (Lanzar instancias).

2. Adjuntar el volumen a la instancia temporal como volumen secundario de la siguiente manera:

   a. En el panel de navegación, elija Volumes (Volúmenes), seleccione el volumen que desconectó de la instancia original y, luego, elija Actions (Acciones), Detach Volume (Adjuntar volumen).

   b. En el cuadro de diálogo, Attach Volume (Adjuntar volumen), para Instances (Instancias), comience a escribir el nombre o el ID de la instancia temporal y, a continuación, seleccione la instancia de la lista.

c. Para Device (Dispositivo), escriba **xvdf** (si aún no está allí) y, luego, elija Attach (Adjuntar).

Paso 4: Eliminar el archivo .run-once

Ahora debe eliminar el archivo `.run-once` del volumen sin conexión adjunto a la instancia. Esto indica a EC2Launch v2 que ejecute todas las tareas con una frecuencia de `once`, lo que incluye establecer la contraseña de administrador. La ruta del archivo en el volumen secundario que adjuntó será similar a `D:\ProgramData\Amazon\EC2Launch\state\.run-once`.

Para eliminar el archivo .run-once

1. Abra la utilidad Administración de discos y lleve el disco online con las siguientes instrucciones: Hacer que un volumen de Amazon EBS esté disponible para su uso.
2. Localice el archivo `.run-once` en el disco que puso en línea.
3. Elimine el archivo .run-once.

> **Important**
>
> Esta acción desencadenará cualquier script configurado para ejecutarse una vez.

Paso 5: Reiniciar la instancia original

Después de haber eliminado el archivo `.run-once`, vuelva a asociar el volumen a la instancia original como volumen raíz y conéctese a la instancia utilizando su par de claves para recuperar la contraseña de administrador.

1. Vuelva a adjuntar el volumen a la instancia original de la siguiente manera:

   a. En el panel de navegación, elija Volumes (Volúmenes), seleccione el volumen que desconectó de la instancia original y, luego, elija Actions (Acciones), Detach Volume (Adjuntar volumen).

   b. En el cuadro de diálogo, Attach Volume (Adjuntar volumen), para Instances (Instancias), comience a escribir el nombre o el ID de la instancia temporal y, a continuación, seleccione la instancia de la lista.

   c. Para Device (Dispositivo), escriba **/dev/sda1**.

d. Elija Attach (Adjuntar). Una vez que el estado del volumen cambie a `in-use`, proceda con el siguiente paso.

2. En el panel de navegación, seleccione Instances (Instancias). Seleccione la instancia original y elija Instance state (Estado de la instancia) y, luego, Start instance (Iniciar instancia). Una vez que el estado de la instancia cambie a `Running`, proceda con el siguiente paso.
3. Recupere su nueva contraseña de administrador de Windows mediante la clave privada del nuevo par de claves y conéctese a la instancia. Para obtener más información, consulte Conexión con la instancia de Windows de.

> **Important**
>
> La instancia recibe una dirección IP pública nueva cuando la para y la comienza. Asegúrese de conectar la instancia utilizando su nombre de DNS público actual. Para obtener más información, consulte Ciclo de vida de la instancia.

4. (Opcional) Puede terminar la instancia temporal cuando no vaya a utilizarla más. Seleccione la instancia temporal y elija Instance state (Estado de la instancia) y Terminate instance (Terminar instancia).

Restablecer la contraseña de administrador de Windows mediante EC2Config

Si perdió su contraseña de administrador de Windows y utiliza una AMI de Windows anterior a Windows Server 2016, puede utilizar el agente EC2Config para generar una contraseña nueva.

Si utiliza una AMI de Windows Server 2016 o una versión posterior, consulte Restablecer la contraseña de administrador de Windows mediante EC2Launch o bien, puede utilizar la herramienta EC2Rescue, que emplea el servicio EC2Launch para generar una nueva contraseña.

> **Note**
>
> Si ha deshabilitado la cuenta de administrador local en la instancia y esta está configurada para Systems Manager, también puede volver a habilitar y restablecer la contraseña de administrador local por medio de EC2Rescue y Run Command. Para obtener más información, consulte Uso de EC2Rescue para Windows Server con Systems Manager Run Command.

> **Note**
>
> Existe un documento de automatización de AWS Systems Manager que aplica de manera automática los pasos manuales necesarios para restablecer la contraseña del administrador local. Para obtener más información, consulte Restablecimiento de contraseñas y claves de SSH en instancias de EC2 en la Guía del usuario de AWS Systems Manager.

Para restablecer la contraseña de administrador de Windows utilizando EC2Config, debe hacer lo siguiente:

- Paso 1: Comprobar que el servicio EC2Config se está ejecutando
- Paso 2: Separar el volumen raíz de la instancia
- Paso 3: Adjuntar el volumen a una instancia temporal
- Paso 4: Modificar el archivo de configuración
- Paso 5: Reiniciar la instancia original

Paso 1: Comprobar que el servicio EC2Config se está ejecutando

Antes de intentar restablecer la contraseña de administrador, verifique que el servicio EC2Config está instalado y en ejecución. Utilizará el servicio EC2Config para restablecer la contraseña de administrador más adelante en esta sección.

Para comprobar que el servicio EC2Config se está ejecutando

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancias) y luego, la instancia que necesita restablecer la contraseña. Esta instancia se denomina instancia original en este procedimiento.
3. (Consola nueva) Elija Actions (Acciones), Monitor and troubleshoot (Supervisión y solución de problemas), Get system log (Obtener registro del sistema).

   (Consola antigua) Elija Actions (Acciones), System Settings (Configuración del sistema), Get System Log (Obtener registro del sistema).
4. Localice la entrada de EC2 Agent, por ejemplo, EC2 Agent: Ec2Config service v3.18.1118. Si ve esta entrada, el servicio EC2Config está ejecutándose.

Si el resultado del registro del sistema está vacío o si el servicio EC2Config no se está ejecutando, solucione los problemas de la instancia usando el servicio de capturas de pantalla de consola de instancia. Para obtener más información, consulte Captura de pantalla de una instancia inaccesible.

Paso 2: Separar el volumen raíz de la instancia

No puede utilizar el servicio EC2Config para restablecer una contraseña de administrador si el volumen donde se almacena la contraseña está vinculado a una instancia como volumen raíz. Debe separar el volumen de la instancia original para que pueda adjuntarlo a una instancia temporal como volumen secundario.

Desconectar el volumen raíz de la instancia

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Seleccione la instancia que requiere el restablecimiento de la contraseña y elija Estado de instancia, Detener instancia. Después de que el estado de la instancia cambie a Stopped (Detenido), proceda con el siguiente paso.
4. (Opcional) Si dispone de la clave privada que especificó cuando lanzó esta instancia, proceda con el siguiente paso. De lo contrario, siga los pasos siguientes para reemplazar la instancia por una nueva que se lance con un nuevo par de claves.

    a. Cree un nuevo par de claves mediante la consola de Amazon EC2. Si desea dar al nuevo par de claves el mismo nombre que tenía la clave privada que perdió, primero debe eliminar el par de claves existente.

    b. Seleccione la instancia que desea reemplazar. Tenga en cuenta el tipo de instancia, la VPC, la subred, el grupo de seguridad y el rol de IAM de la instancia.

    c. Elija Actions (Acciones), Image and templates (Imagen y plantillas), Create image (Crear imagen). Escriba un nombre y una descripción para la imagen y, luego, elija Create image (Crear imagen). En el panel de navegación, elija AMIs. Una vez que el estado de la imagen cambie a available (disponible), proceda con el paso siguiente.

    d. Seleccione la imagen y elija Actions (Acciones) y, a continuación, Launch (Lanzar).

e. Complete el asistente con el mismo tipo de instancia, VPC, subred, grupo de seguridad y rol de IAM que la instancia que se desea reemplazar y, a continuación, seleccione Launch (Lanzar).

f. Cuando se solicite, elija el par de claves que creó para la nueva instancia, seleccione la casilla de confirmación y, a continuación, elija Launch Instances (Lanzar instancias).

g. (Opcional) Si la instancia original tenía una dirección IP elástica asociada, transfiérala a la nueva instancia. Si la instancia original tiene volúmenes de EBS además del volumen raíz, transfiéralos a la nueva instancia.

5. Desconecte el volumen raíz de la instancia original de la siguiente manera:

   a. Seleccione la instancia original y elija la pestaña Almacenamiento. Anote el nombre del dispositivo raíz en Nombre del dispositivo raíz. Busque el volumen con el nombre de este dispositivo en Dispositivos de bloques y anote el ID del volumen.

   b. En el panel de navegación, elija Volumes (Volúmenes).

   c. En la lista de volúmenes, seleccione el volumen que anotó como dispositivo raíz y elija Acciones, Separar volumen. Una vez que el estado del volumen cambie a available (disponible), siga con el paso siguiente.

6. Si creó una instancia nueva para reemplazar la instancia original, puede terminar la original ahora. Ya no se necesita. Para el resto del procedimiento, todas las referencias a la instancia original se aplican a la que acaba de crear.

Paso 3: Adjuntar el volumen a una instancia temporal

A continuación, lance una instancia temporal y adjúntele el volumen como volumen secundario. Esta es la instancia que debe utilizar para modificar el archivo de configuración.

Para lanzar una instancia temporal y adjuntar el volumen

1. Lance la instancia temporal de la siguiente manera:

   a. En el panel de navegación, elija Instances (Instancias), luego elija Launch instances (Lanzar instancias) y por último, seleccione una AMI.

   > **Important**
   >
   > Es necesario seleccionar una AMI para una versión diferente de Windows a fin de impedir que se produzcan conflictos de firmas de disco. Por ejemplo, si la instancia

original ejecuta Windows Server 2019, lance la instancia temporal mediante el uso de una AMI para Windows Server 2016.

b. Mantenga el tipo de instancia predeterminada y, a continuación, seleccione Next: Configure Instance Details (Siguiente: Configurar detalles de la instancia).

c. En la página Configure Instance Details (Configurar detalles de la instancia), para Subred, seleccione la misma zona de disponibilidad que la de la instancia original y elija Review and Launch (Revisar y lanzar).

> **Important**
>
> La instancia temporal debe estar en la misma zona de disponibilidad que la instancia original. Si su instancia temporal se encuentra en una zona de disponibilidad diferente, no podrá adjuntar a ella el volumen raíz de la instancia original.

d. En la página Review Instance Launch, elija Launch.

e. Cuando lo solicite, cree un nuevo par de claves, descárguelas en un lugar seguro de su computadora y, a continuación, elija Launch Instances (Lanzar instancias).

2. Adjuntar el volumen a la instancia temporal como volumen secundario de la siguiente manera:

a. En el panel de navegación, elija Volumes (Volúmenes), seleccione el volumen que desconectó de la instancia original y, luego, elija Actions (Acciones), Detach Volume (Adjuntar volumen).

b. En el cuadro de diálogo, Attach Volume (Adjuntar volumen), para Instances (Instancias), comience a escribir el nombre o el ID de la instancia temporal y, a continuación, seleccione la instancia de la lista.

c. Para Device (Dispositivo), escriba **`xvdf`** (si aún no está allí) y, luego, elija Attach (Adjuntar).

Paso 4: Modificar el archivo de configuración

Después de adjuntar el volumen a una instancia temporal como volumen secundario, modifique el complemento `Ec2SetPassword` en el archivo de configuración.

Para modificar el archivo de configuración

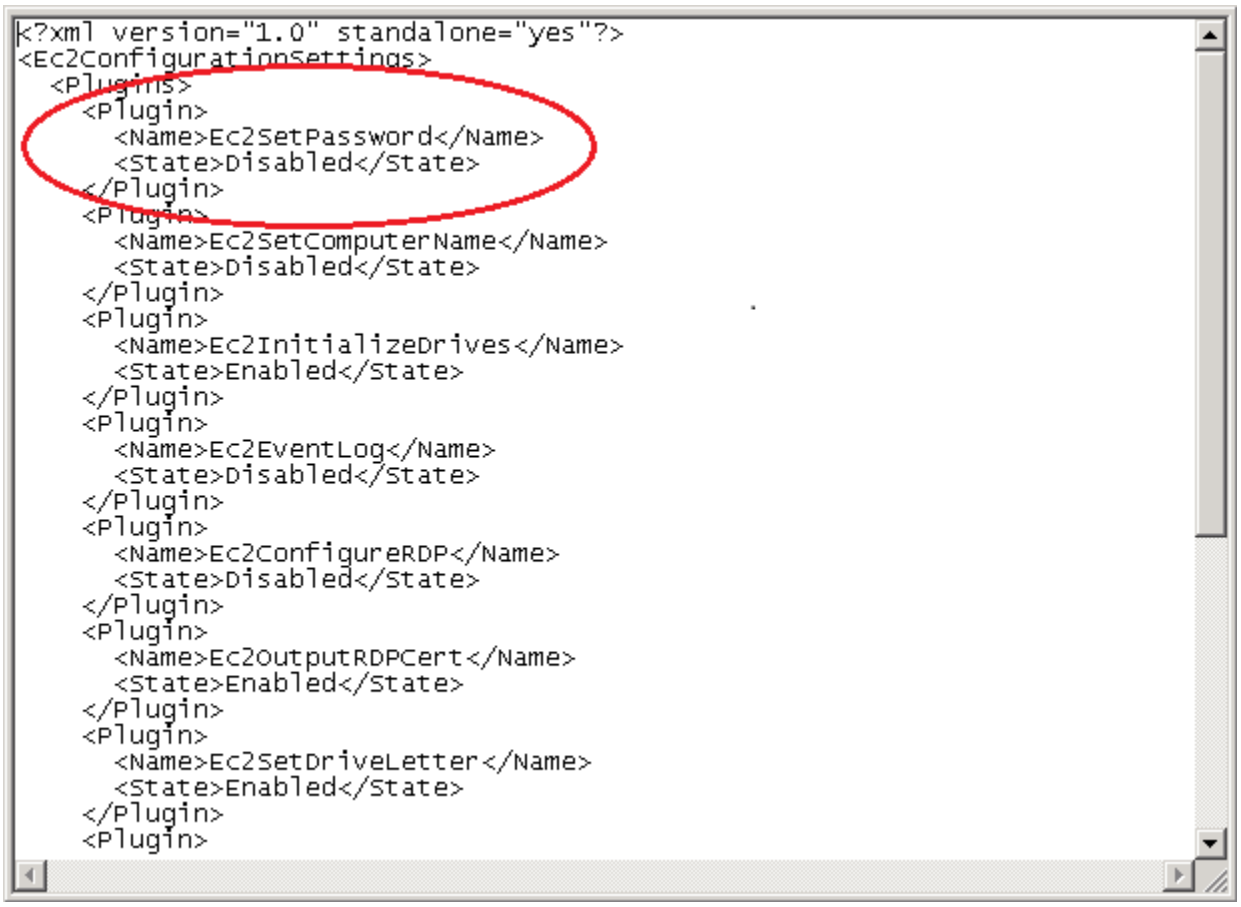
1. En la instancia temporal, modifique el archivo de configuración en el volumen secundario del modo siguiente:

   a. Lance y conéctese a la instancia temporal.

   b. Siga las instrucciones a continuación para poner la unidad en línea: Ponga un volumen de Amazon EBS a disposición para su uso.

   c. Desplácese hasta el volumen secundario y abra `\Program Files\Amazon \Ec2ConfigService\Settings\config.xml` con un editor de texto, como el Bloc de notas.

   d. En la parte superior del archivo, busque el complemento con el nombre `Ec2SetPassword`, tal como se muestra en la captura de pantalla. Cambie el estado de `Disabled` a `Enabled` y guarde el archivo.



2. Después de modificar el archivo de configuración, separe el volumen secundario de la instancia temporal del modo siguiente:

a. Mediante la utilidad Disk Management (Administración de discos), desconecte el volumen.
b. Desconéctese de la instancia temporal y vuelva a la consola de Amazon EC2.
c. En el panel de navegación, elija Volumes (Volúmenes), seleccione el volumen y luego elija Actions (Acciones), Detach Volume (Separar volumen). Una vez que el estado del volumen cambie a available (disponible), siga con el paso siguiente.

Paso 5: Reiniciar la instancia original

Después de modificar el archivo de configuración, adjunte el volumen de nuevo a la instancia original como volumen raíz y conéctese a la instancia utilizando su par de claves para recuperar la contraseña de administrador.

1. Vuelva a adjuntar el volumen a la instancia original de la siguiente manera:
   a. En el panel de navegación, elija Volumes (Volúmenes), seleccione el volumen que desconectó de la instancia original y, luego, elija Actions (Acciones), Detach Volume (Adjuntar volumen).
   b. En el cuadro de diálogo, Attach Volume (Adjuntar volumen), para Instances (Instancias), comience a escribir el nombre o el ID de la instancia temporal y, a continuación, seleccione la instancia de la lista.
   c. Para Device (Dispositivo), escriba **`/dev/sda1`**.
   d. Elija Attach (Adjuntar). Una vez que el estado del volumen cambie a `in-use`, proceda con el siguiente paso.
2. En el panel de navegación, seleccione Instances (Instancias). Seleccione la instancia original y elija Instance state (Estado de la instancia) y, luego, Start instance (Iniciar instancia). Una vez que el estado de la instancia cambie a `Running`, proceda con el siguiente paso.
3. Recupere su nueva contraseña de administrador de Windows mediante la clave privada del nuevo par de claves y conéctese a la instancia. Para obtener más información, consulte Conexión con la instancia de Windows de.

> **Important**
>
> La instancia recibe una dirección IP pública nueva cuando la para y la comienza. Asegúrese de conectar la instancia utilizando su nombre de DNS público actual. Para obtener más información, consulte Ciclo de vida de la instancia.

4. (Opcional) Puede terminar la instancia temporal cuando no vaya a utilizarla más. Seleccione la instancia temporal y elija Instance state (Estado de la instancia) y Terminate instance (Terminar instancia).

Restablecer la contraseña de administrador de Windows mediante EC2Launch

Si perdió su contraseña de administrador de Windows y utiliza una AMI de Windows Server 2016 o una versión posterior, puede utilizar la herramienta EC2Rescue, que emplea el servicio EC2Launch para generar una nueva contraseña.

Si usa una AMI de Windows Server 2016 o posterior que no incluye el agente EC2Launch v2, puede usar EC2Launch v2 para generar una contraseña nueva.

Si está utilizando una AMI de Windows Server anterior a Windows Server 2016, consulte Restablecer la contraseña de administrador de Windows mediante EC2Config.

> **Warning**
>
> Cuando detiene una instancia, se borran los datos contenidos en todos los volúmenes de almacén de instancias. Para conservar los datos de los volúmenes del almacén de instancias, asegúrese de realizar una copia de seguridad de ellos en un almacenamiento persistente.

> **Note**
>
> Si ha deshabilitado la cuenta de administrador local en la instancia y esta está configurada para Systems Manager, también puede volver a habilitar y restablecer la contraseña de administrador local por medio de EC2Rescue y Run Command. Para obtener más información, consulte Uso de EC2Rescue para Windows Server con Systems Manager Run Command.

> **Note**
>
> Existe un documento de automatización de AWS Systems Manager que aplica de manera automática los pasos manuales necesarios para restablecer la contraseña del administrador

local. Para obtener más información, consulte Restablecimiento de contraseñas y claves de SSH en instancias de EC2 en la Guía del usuario de AWS Systems Manager.

Para restablecer la contraseña de administrador de Windows utilizando EC2Launch, debe hacer lo siguiente:

- Paso 1: Separar el volumen raíz de la instancia
- Paso 2: Adjuntar el volumen a una instancia temporal
- Paso 3: Restablecer la contraseña de administrador
- Paso 4: Reiniciar la instancia original

Paso 1: Separar el volumen raíz de la instancia

No puede utilizar el servicio EC2Launch para restablecer una contraseña de administrador si el volumen donde se almacena la contraseña está vinculado a una instancia como volumen raíz. Debe separar el volumen de la instancia original para que pueda adjuntarlo a una instancia temporal como volumen secundario.

Desconectar el volumen raíz de la instancia

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Seleccione la instancia que requiere el restablecimiento de la contraseña y elija Estado de instancia, Detener instancia. Después de que el estado de la instancia cambie a Stopped (Detenido), proceda con el siguiente paso.
4. (Opcional) Si dispone de la clave privada que especificó cuando lanzó esta instancia, proceda con el siguiente paso. De lo contrario, siga los pasos siguientes para reemplazar la instancia por una nueva que se lance con un nuevo par de claves.

    a. Cree un nuevo par de claves mediante la consola de Amazon EC2. Si desea dar al nuevo par de claves el mismo nombre que tenía la clave privada que perdió, primero debe eliminar el par de claves existente.

    b. Seleccione la instancia que desea reemplazar. Tenga en cuenta el tipo de instancia, la VPC, la subred, el grupo de seguridad y el rol de IAM de la instancia.

c. Elija Actions (Acciones), Image and templates (Imagen y plantillas), Create image (Crear imagen). Escriba un nombre y una descripción para la imagen y, luego, elija Create image (Crear imagen). En el panel de navegación, elija AMIs. Una vez que el estado de la imagen cambie a available (disponible), proceda con el paso siguiente.

d. Seleccione la imagen y elija Actions (Acciones) y, a continuación, Launch (Lanzar).

e. Complete el asistente con el mismo tipo de instancia, VPC, subred, grupo de seguridad y rol de IAM que la instancia que se desea reemplazar y, a continuación, seleccione Launch (Lanzar).

f. Cuando se solicite, elija el par de claves que creó para la nueva instancia, seleccione la casilla de confirmación y, a continuación, elija Launch Instances (Lanzar instancias).

g. (Opcional) Si la instancia original tenía una dirección IP elástica asociada, transfiérala a la nueva instancia. Si la instancia original tiene volúmenes de EBS además del volumen raíz, transfiéralos a la nueva instancia.

5. Desconecte el volumen raíz de la instancia original de la siguiente manera:

   a. Seleccione la instancia original y elija la pestaña Almacenamiento. Anote el nombre del dispositivo raíz en Nombre del dispositivo raíz. Busque el volumen con el nombre de este dispositivo en Dispositivos de bloques y anote el ID del volumen.

   b. En el panel de navegación, elija Volumes (Volúmenes).

   c. En la lista de volúmenes, seleccione el volumen que anotó como dispositivo raíz y elija Acciones, Separar volumen. Una vez que el estado del volumen cambie a available (disponible), siga con el paso siguiente.

6. Si creó una instancia nueva para reemplazar la instancia original, puede terminar la original ahora. Ya no se necesita. Para el resto del procedimiento, todas las referencias a la instancia original se aplican a la que acaba de crear.

Paso 2: Adjuntar el volumen a una instancia temporal

A continuación, lance una instancia temporal y adjúntele el volumen como volumen secundario. Es la instancia que utiliza para ejecutar EC2Launch.

Para lanzar una instancia temporal y adjuntar el volumen

1. Lance la instancia temporal de la siguiente manera:

a. En el panel de navegación, elija Instances (Instancias), luego elija Launch instances (Lanzar instancias) y por último, seleccione una AMI.

> **Important**
>
> Es necesario seleccionar una AMI para una versión diferente de Windows a fin de impedir que se produzcan conflictos de firmas de disco. Por ejemplo, si la instancia original ejecuta Windows Server 2019, lance la instancia temporal mediante el uso de una AMI para Windows Server 2016.

b. Mantenga el tipo de instancia predeterminada y, a continuación, seleccione Next: Configure Instance Details (Siguiente: Configurar detalles de la instancia).

c. En la página Configure Instance Details (Configurar detalles de la instancia), para Subred, seleccione la misma zona de disponibilidad que la de la instancia original y elija Review and Launch (Revisar y lanzar).

> **Important**
>
> La instancia temporal debe estar en la misma zona de disponibilidad que la instancia original. Si su instancia temporal se encuentra en una zona de disponibilidad diferente, no podrá adjuntar a ella el volumen raíz de la instancia original.

d. En la página Review Instance Launch, elija Launch.

e. Cuando lo solicite, cree un nuevo par de claves, descárguelas en un lugar seguro de su computadora y, a continuación, elija Launch Instances (Lanzar instancias).

2. Adjuntar el volumen a la instancia temporal como volumen secundario de la siguiente manera:

a. En el panel de navegación, elija Volumes (Volúmenes), seleccione el volumen que desconectó de la instancia original y, luego, elija Actions (Acciones), Detach Volume (Adjuntar volumen).

b. En el cuadro de diálogo, Attach Volume (Adjuntar volumen), para Instances (Instancias), comience a escribir el nombre o el ID de la instancia temporal y, a continuación, seleccione la instancia de la lista.

c. Para Device (Dispositivo), escriba **`xvdf`** (si aún no está allí) y, luego, elija Attach (Adjuntar).

Paso 3: Restablecer la contraseña de administrador

A continuación, conéctese a la instancia temporal y utilice EC2Launch para restablecer la contraseña de administrador.

Para restablecer la contraseña del administrador

1. Establezca conexión con la instancia temporal y use la herramienta EC2Rescue for Windows Server de la instancia para restablecer la contraseña de administrador tal y como se indica a continuación:

   a. Descargue el archivo zip EC2Rescue for Windows Server, extraiga su contenido y ejecute EC2Rescue.exe.

   b. En la pantalla License Agreement (Contrato de licencia), lea el contrato de licencia y, si acepta los términos, marque I Agree (Acepto).

   c. En la pantalla Welcome to EC2Rescue for Windows Server(Bienvenido a EC2Rescue for Windows Server), elija Next (Siguiente).

   d. En la pantalla Select mode (Seleccionar modo), elija Offline instance (Instancia sin conexión).

   e. En la pantalla Select a disk (Seleccionar un disco), seleccione el dispositivo xvdf y elija Next (Siguiente).

   f. Confirme la selección del disco y elija Yes (Sí).

   g. Una vez cargado el volumen, elija OK (Aceptar).

   h. En la pantalla Select Offline Instance Option (Seleccionar opción de instancia sin conexión), elija Diagnose and Rescue (Diagnosticar y rescatar).

   i. En la pantalla Summary (Resumen), compruebe la información y elija Next (Siguiente).

   j. En la pantalla Detected possible issues (Posibles problemas detectados), seleccione Reset Administrator Password (Restablecer contraseña de administrador) y elija Next (Siguiente).

   k. En la pantalla Confirm (Confirmar), elija Rescue (Rescatar), OK (Aceptar).

   l. En la pantalla Done (Listo), elija Finish (Finalizar).

   m. Cierre la herramienta EC2Rescue for Windows Server, desconéctese de la instancia temporal y luego vuelva a la consola de Amazon EC2.

2. Separe el volumen (`xvdf`) secundario de la instancia temporal como sigue:

   a. En el panel de navegación, elija Instances (Instancias) y seleccione la instancia temporal.

b. En la pestaña Storage (Almacenamiento) de la instancia temporal, observe el ID del volumen EBS que aparece como xvdf.

c. En el panel de navegación, elija Volumes (Volúmenes).

d. En la lista de volúmenes, seleccione el volumen indicado en el paso anterior y elija Actions (Acciones), Detach Volume (Separar volumen). Una vez que el estado del volumen cambie a available (disponible), siga con el paso siguiente.

Paso 4: Reiniciar la instancia original

Después de restablecer la contraseña de administrador mediante EC2Launch, adjunte el volumen de nuevo a la instancia original como volumen raíz y conéctese a la instancia utilizando su par de claves para recuperar la contraseña de administrador.

Para reiniciar la instancia original

1. Vuelva a adjuntar el volumen a la instancia original de la siguiente manera:

   a. En el panel de navegación, elija Volumes (Volúmenes), seleccione el volumen que desconectó de la instancia original y, luego, elija Actions (Acciones), Detach Volume (Adjuntar volumen).

   b. En el cuadro de diálogo, Attach Volume (Adjuntar volumen), para Instances (Instancias), comience a escribir el nombre o el ID de la instancia temporal y, a continuación, seleccione la instancia de la lista.

   c. Para Device (Dispositivo), escriba **`/dev/sda1`**.

   d. Elija Attach (Adjuntar). Una vez que el estado del volumen cambie a `in-use`, proceda con el siguiente paso.

2. En el panel de navegación, seleccione Instances (Instancias). Seleccione la instancia original y elija Instance state (Estado de la instancia) y, luego, Start instance (Iniciar instancia). Una vez que el estado de la instancia cambie a `Running`, proceda con el siguiente paso.

3. Recupere su nueva contraseña de administrador de Windows mediante la clave privada del nuevo par de claves y conéctese a la instancia. Para obtener más información, consulte Conexión con la instancia de Windows de.

4. (Opcional) Puede terminar la instancia temporal cuando no vaya a utilizarla más. Seleccione la instancia temporal y elija Instance state (Estado de la instancia) y Terminate instance (Terminar instancia).

Solución de problemas de una instancia inaccesible

Puede utilizar los métodos siguientes para solución de problemas de una instancia de Amazon EC2 inaccesible.

Contenido

Reinicio de la instancia

La capacidad para reiniciar instancias que de otro modo son inaccesibles es valiosa para solucionar problemas y para la administración de instancia general.

Al igual que puede reiniciar el equipo presionando el botón de restablecer, puede hacer lo mismo con las instancias de EC2 mediante la CLI, la API o la consola de Amazon EC2. Para obtener más información, consulte Reinicio de su instancia.

Salida de la consola de instancias

El resultado de la consola es una herramienta valiosa en el diagnóstico de problemas. Es especialmente útil para solucionar problemas del kernel y de configuración de servicio que podrían causar la terminación de una instancia o hacer que fuera inalcanzable antes de poder iniciar su daemon SSH.

- Instancias de Linux: la salida de la consola de instancias muestra la salida exacta de la consola que se mostraría normalmente en un monitor físico conectado a un equipo. La salida de la consola devuelve información almacenada en el búfer que se publicó justo después de un estado de transición de la instancia (iniciar, detener, reiniciar y terminar). El resultado publicado no se actualiza de forma continua, sino solo cuando es probable que tenga más valor.
- Instancias de Windows: la salida de la consola de la instancia incluye los tres últimos errores del registro de eventos del sistema.

Como opción, puede recuperar la salida más reciente de la consola serie en cualquier momento durante el ciclo de vida de la instancia. Esta opción solo se admite en las instancias integradas en el AWS Nitro System. No se admite a través de la consola de Amazon EC2.

> **Note**
>
> Solo se almacenan los 64 KB más recientes de la salida publicada, que está disponible por lo menos durante una hora después de la última publicación.

Únicamente el propietario de la instancia tiene acceso a la salida de la consola.

Utilice uno de los siguientes métodos para obtener el resultado de la consola.

Console

Para obtener el resultado de la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación izquierdo, elija instancias.
3. Seleccione la instancia y luego elija Acciones, Monitorear y solucionar problemas, Obtener registro del sistema.

Command line

Para obtener el resultado de la consola

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

- get-console-output (AWS CLI)
- Get-EC2ConsoleOutput (AWS Tools for Windows PowerShell)

Captura de pantalla de una instancia inaccesible

Si no puede conectarse a la instancia, puede hacer una captura de pantalla de la instancia y verla como una imagen. La imagen puede ofrecer visibilidad del estado de la instancia y permite solucionar los problemas más rápidamente.

Puede generar capturas de pantalla mientras se ejecuta la instancia o después de que se haya bloqueado. La imagen se genera en formato JPG y no es superior a 100 kb. No hay costo de trasferencia de datos por la captura de pantalla.

Limitaciones

Esta característica no es compatible para lo siguiente:

- Instancias bare metal (instancias de tipo `*.metal`)
- La instancia utiliza un controlador NVIDIA GRID
- Instancias equipadas con procesadores Graviton basados en ARM
- Instancias de Windows en AWS Outposts

Regiones admitidas

Esta característica está disponible en las siguientes regiones de :

- US East (N. Virginia) Region
- Región del este de EE. UU. (Ohio)
- Región del oeste de EE. UU. (Norte de California)
- Región del oeste de EE. UU. (Oregón)
- Región África (Ciudad del Cabo)
- Región de Asia-Pacífico (Hong Kong)
- Región de Asia Pacífico (Hyderabad)
- Región Asia-Pacífico (Yakarta)
- Región de Asia-Pacífico (Melbourne)
- Región de Asia-Pacífico (Bombay)
- Región Asia-Pacífico (Osaka)
- Región de Asia-Pacífico (Seúl)
- Región de Asia-Pacífico (Singapur)
- Región de Asia-Pacífico (Sídney)
- Asia Pacífico (Tokio)
- Región de Canadá (centro)
- Región del oeste de Canadá (Calgary)

- Región China (Pekín)
- Región China (Ningxia)
- Región de Europa (Fráncfort)
- Región de Europa (Irlanda)
- Región de Europa (Londres)
- Región Europa (Milán)
- Región Europa (París)
- Región Europa (España)
- Región Europa (Estocolmo)
- Región Europa (Zúrich)
- Región Israel (Tel Aviv)
- Región de América del Sur (São Paulo)
- Región Medio Oriente (Baréin)
- Región Medio Oriente (EAU)

Console

Hacer una captura de pantalla de una instancia

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación izquierdo, elija Instances.
3. Seleccione la instancia que va a capturar.
4. Selecciona Acciones, luego selecciona Supervisar y solucionar problemas y a continuación selecciona Obtener captura de pantalla de instancia.
5. Selecciona Descargaro haz clic con el botón derecho en la imagen para descargarla y guardarla.

Command line

Hacer una captura de pantalla de una instancia

Puede utilizar uno de los siguientes comandos. El contenido devuelto está codificado en base64. Para obtener más información acerca de estas interfaces de línea de comandos, consulte Acceder a Amazon EC2.

- get-console-screenshot (AWS CLI)
- GetConsoleScreenshot (API de consultas de Amazon EC2)

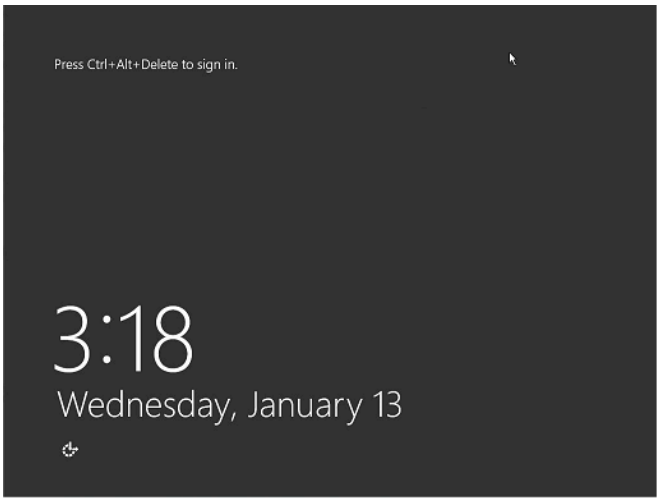
Capturas de pantalla comunes para las instancias de Windows

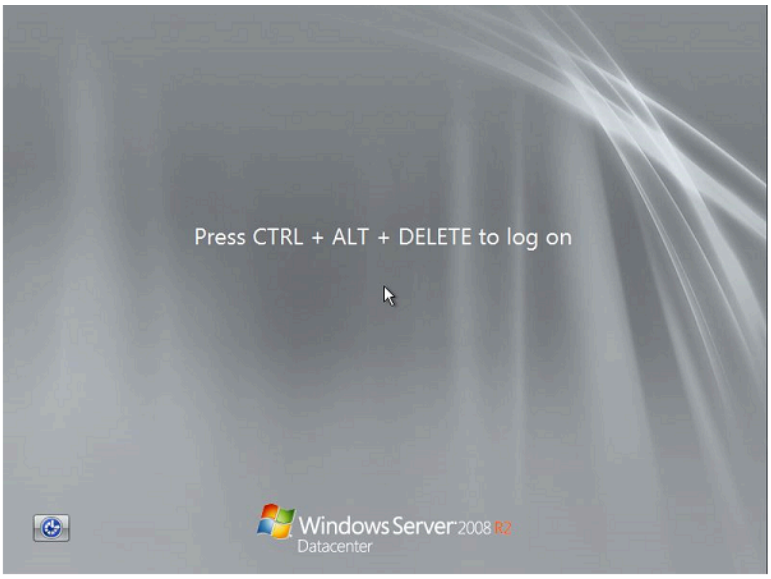
Puede usar la siguiente información para ayudarlo a solucionar problemas de instancias de inaccesibles de Windows en función de las capturas de pantalla que devuelve el servicio.

- Pantalla de inicio de sesión (Ctrl+Alt+Supr)
- Pantalla de recuperación de la consola
- Pantalla Windows Boot Manager
- Pantalla Sysprep
- Pantalla Getting Ready
- Pantalla Windows Update
- Chkdsk

Pantalla de inicio de sesión (Ctrl+Alt+Supr)

El servicio de captura de pantalla de la consola devolvió lo siguiente.





Si una instancia resulta inaccesible durante el inicio de sesión, podría existir un problema con la configuración de red o los Servicios de Escritorio remoto de Windows. Una instancia también puede no dar respuesta si algún proceso está usando grandes cantidades de CPU.

Configuración de red

Use la siguiente información para comprobar que sus configuraciones AWSde red local (o en las instalaciones) y Microsoft Windows no estén bloqueando el acceso a la instancia.

Configuración de la red de AWS

Configuración	Verificar
Configuración del grupo de seguridad	Verifique que el puerto 3389 está abierto para el grupo de seguridad. Verifique que se ha conectado a la dirección IP pública correcta. Si la instancia no se asoció a una dirección IP elástica, la dirección IP pública cambia después de que la instancia se detenga o se inicie. Para obtener más información, consulte El escritorio remoto no puede conectarse al equipo remoto.
Configuración de VPC (ACL de red)	Verifique que la lista de control de acceso (ACL) para la Amazon VPC no está bloqueando el acceso. Para obtener información, consulte ACL de red en la Guía del usuario de Amazon VPC.
Configuración de la VPN	Si se está conectando a la VPC usando una red privada virtual (VPN), verifique la conexión de túnel de la VPN. Para obtener más información, consulte el tema sobre cómo solucionar problemas relacionados con la conectividad del túnel de VPN a una Amazon VPC.

Configuración de red de Windows

Configuración	Verificar
Firewall de Windows	Verifique que el firewall de Windows no está bloqueando las conexiones con la instancia . Deshabilite el firewall de Windows como

Configuración	Verificar
	se describe en el punto 7 de la sección de solución de problemas de escritorio remoto, El escritorio remoto no puede conectarse al equipo remoto.
Configuración TCP/IP avanzada (Uso de IP estática)	La instancia puede no responder porque se ha configurado una dirección IP estática. En una VPC, cree una interfaz de red y asóciela a la instancia.

Configuración de red local/en las instalaciones

Verifique que la configuración de red local no está bloqueando el acceso. Intente conectarse a otra instancia de la misma VPC que la instancia inaccesible. Si no puede obtener acceso a otra instancia, trabaje con el administrador de red local para determinar si existe una política local que restringe el acceso.

Problema con los servicios de Escritorio remoto

Si la instancia no se puede alcanzar durante el inicio de sesión, podría deberse a un problema con los servicios de Escritorio remoto (RDS) en la instancia.

> **Tip**
>
> Puede utilizar el manual de procedimientos de `AWSSupport-TroubleshootRDP` para comprobar y modificar diversas configuraciones que pueden afectar a las conexiones del Protocolo de escritorio remoto (RDP). Para obtener más información, consulte `AWSSupport-TroubleshootRDP` en la Referencia del manual de procedimientos de automatización de AWS Systems Manager.

Configuración del servicio de Escritorio remoto

Configuración	Verificar
RDS se está ejecutando	Verifique que RDS se está ejecutando en la instancia. Conéctese a la instancia usando el complemento de servicios

Configuración	Verificar
	de consola de administración de Microsoft (MMC) (`services.msc`). En la lista de servicios, verifique que Remote Desktop Services (Servicios de Escritorio remoto) está Running (En ejecución). Si no es así, inícielo y después establezca el tipo de inicio en Automatic (Automático). Si no puede conectarse a la instancia con el complemento Services, separe el volumen raíz de la instancia, tome una instantánea del volumen o cree una AMI, adjunte el volumen original a otra instancia de la misma zona de disponibilidad como volumen secundario y modifique la clave Start del registro. Cuando haya terminado, adjunte de nuevo el volumen raíz a la instancia original.
RDS está habilitado.	Aunque el servicio se haya iniciado, es posible que esté deshabilitado. Desconecte el volumen raíz de la instancia, realice una instantánea o cree una AMI del volumen, asocie el volumen original a otra instancia de la misma zona de disponibilidad como un volumen secundario y habilite el servicio modificando la clave Terminal Server del Registro como se describe en Habilitación del escritorio remoto en una instancia de EC2 con el registro remoto. Cuando haya terminado, adjunte de nuevo el volumen raíz a la instancia original.

Uso de CPU elevado

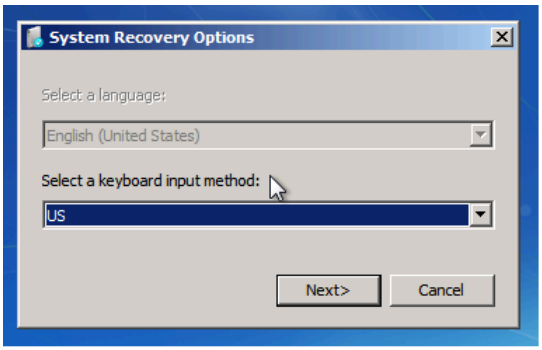
Compruebe la métrica CPUUtilization (Maximum) (Uso de la CPU (máximo)) de la instancia usando Amazon CloudWatch. Si CPUUtilization (Maximum) (Uso de la CPU (máximo)) es un número elevado, espere a que la CPU vaya más lenta e intente volver a conectarse. Un uso elevado de la CPU puede deberse a:

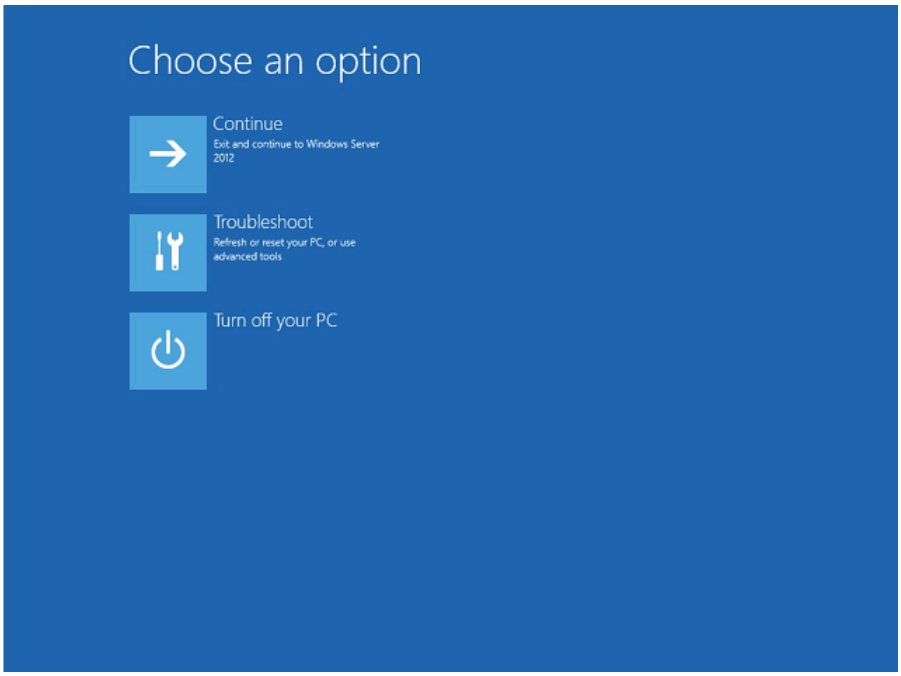
- Actualización de Windows
- Examen de software de seguridad
- Script de inicio personalizado
- Programador de tareas

Para obtener más información, consulte Obtener estadísticas de un recurso específico en la Guía del usuario de Amazon CloudWatch. Para obtener otras sugerencias para la solución de problemas, consulte Elevado uso de la CPU justo después de iniciar Windows (instancias de Windows únicamente).

Pantalla de recuperación de la consola

El servicio de captura de pantalla de la consola devolvió lo siguiente.





El sistema operativo puede arrancar en la consola de recuperación y quedar bloqueado en este estado si `bootstatuspolicy` no está configurado en `ignoreallfailures`. Use el siguiente procedimiento para cambiar la configuración `bootstatuspolicy` a `ignoreallfailures`.

De forma predeterminada, la configuración de la política para las AMI de Windows públicas que proporciona AWS se establece en `ignoreallfailures`.

1. Detenga la instancia inaccesible.
2. Cree una instantánea del volumen raíz. El volumen raíz está adjunto a la instancia como `/dev/sda1`.

   Separe el volumen raíz de la instancia inaccesible, tome una instantánea del volumen o cree una AMI, y adjúntelo a otra instancia de la misma zona de disponibilidad como un volumen secundario.

> **Warning**
>
> Si la instancia temporal se basa en la misma AMI que la instancia original, debe completar otros pasos o no podrá arrancar la instancia original después de restaurar el volumen raíz debido a un conflicto de firmas de disco. Si debe crear una instancia temporal basada en la misma AMI, consulte los pasos en Colisión de firma de disco para evitar un conflicto de firmas de disco.
> Como alternativa, selecciones una AMI diferente para la instancia temporal. Por ejemplo, si la instancia original usa una AMI para Windows Server 2016, lance la instancia temporal usando una AMI para Windows Server 2019.

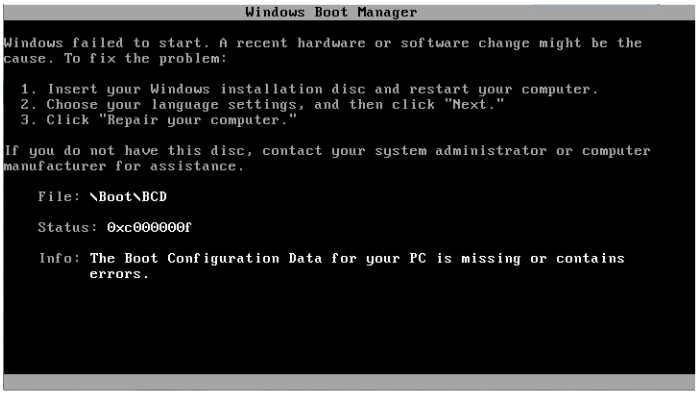
3. Inicia sesión en la instancia y ejecute el siguiente comando desde un comando del sistema para cambiar la configuración `bootstatuspolicy` por `ignoreallfailures`:

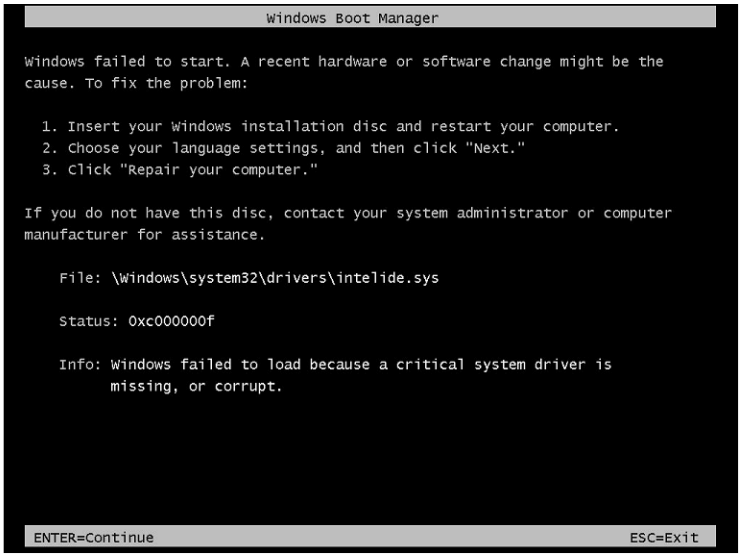
```
bcdedit /store Drive Letter:\boot\bcd /set {default} bootstatuspolicy
 ignoreallfailures
```

4. Vuelva a adjuntar el volumen a la instancia inaccesible e iníciela de nuevo.

Pantalla Windows Boot Manager

El servicio de captura de pantalla de la consola devolvió lo siguiente.



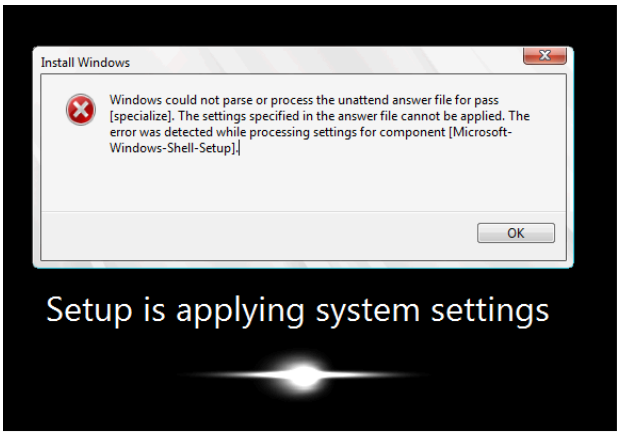


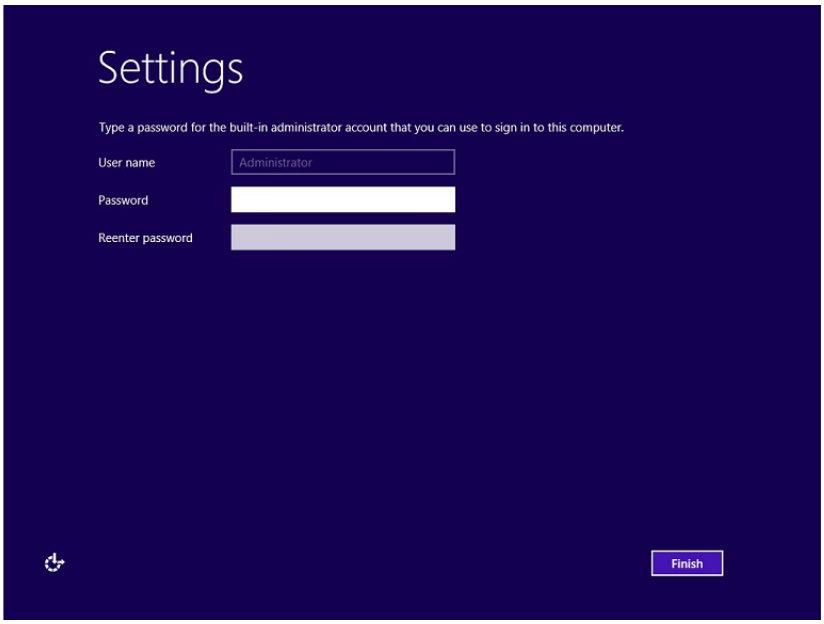
El sistema operativo experimentó un daño irreparable en el archivo del sistema o el Registro. Cuando la instancia se bloquea en este estado, debe recuperarla a partir de una AMI de backup reciente o

lanzar una instancia de sustitución. Si necesita acceso a datos de la instancia, separe los volúmenes raíz de la instancia inaccesible, tome una instantánea de esos volúmenes o cree una AMI a partir de ellos, y adjúntelos a otra instancia de la misma zona de disponibilidad como un volumen secundario.

Pantalla Sysprep

El servicio de captura de pantalla de la consola devolvió lo siguiente.

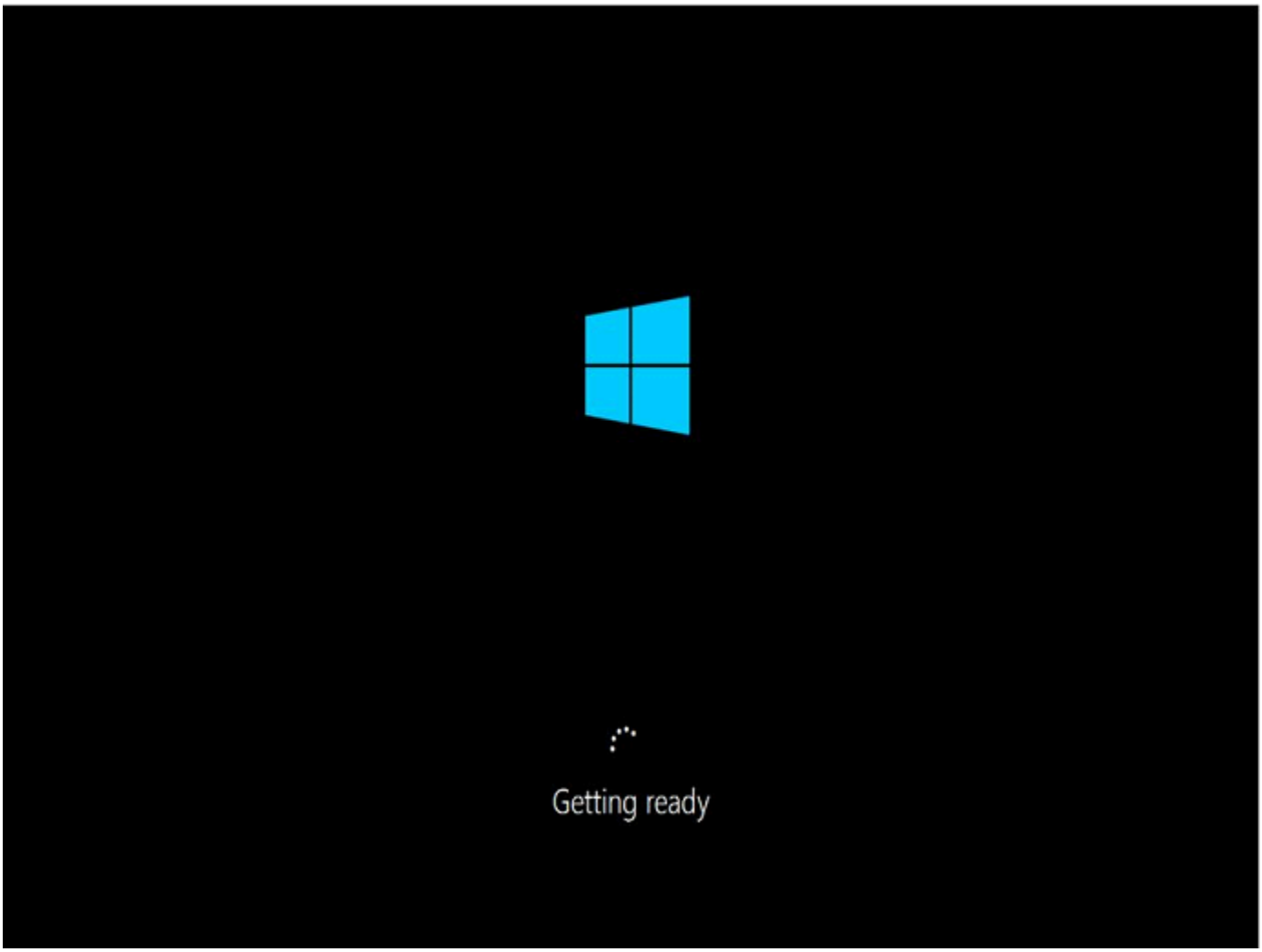




Es posible que vea esta pantalla si no utilizó el servicio EC2Config para llamar a Sysprep o si el sistema operativo dio error al ejecutar Sysprep. Puede restablecer la contraseña con EC2Rescue. De lo contrario, consulte Creación de una AMI con Windows Sysprep.

Pantalla Getting Ready

El servicio de captura de pantalla de la consola devolvió lo siguiente.



Actualice el servicio de captura de pantalla de consola de instancia para verificar que el aro de progreso está girando. Si el aro gira, espere hasta que se inicie el sistema operativo. También puede comprobar la métrica CPUUtilization (Maximum) (Uso de la CPU (máximo)) de la instancia con Amazon CloudWatch para ver si el sistema operativo está activo. Si el aro de progreso no gira, es posible que la instancia se haya bloqueado en el proceso de arranque. Reinicie la instancia. Si el problema no se soluciona, recupere la instancia a partir de una AMI de backup reciente o lance una de sustitución. Si necesita acceso a los datos de la instancia, separe el volumen raíz de la instancia inaccesible, tome una instantánea del volumen o cree una AMI. Después, adjunte el volumen a otra instancia de la misma zona de disponibilidad como un volumen secundario.

Pantalla Windows Update

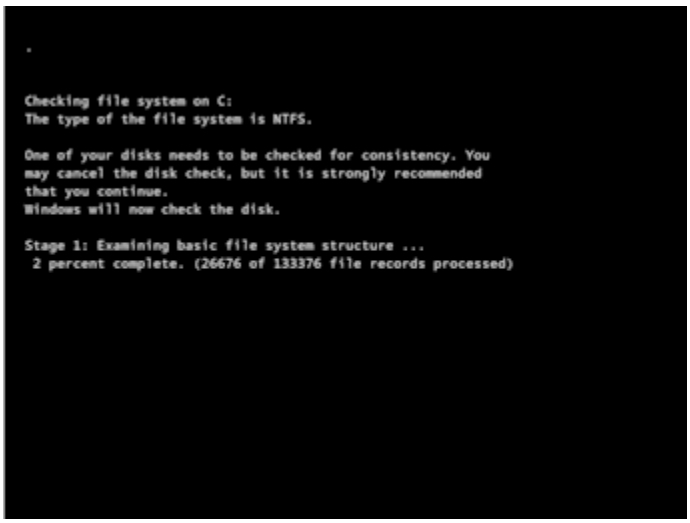
El servicio de captura de pantalla de la consola devolvió lo siguiente.

El proceso de Windows Update está actualizando el Registro. Espere a que finalice la actualización. No arranque ni detenga la instancia pues podrían dañarse los datos durante la actualización.

> **Note**
>
> El proceso de Windows Update puede consumir recursos del servidor durante la actualización. Si experimenta este problema con frecuencia, considere la posibilidad de usar tipos de instancias y volúmenes de EBS más rápidos.

Chkdsk

El servicio de captura de pantalla de la consola devolvió lo siguiente.



Windows está ejecutando la herramienta del sistema chkdsk en la unidad para verificar la integridad del sistema de archivos y corregir errores lógicos. Espere a que el proceso finalice.

Recuperación de instancias cuando el equipo host da error

Si se produce un error irrecuperable en el hardware de un equipo host subyacente, AWS puede programar un evento para detener la instancia. Se le notifica dicho evento antes de que se produzca por correo electrónico.

Recuperación de una instancia respaldada por Amazon EBS que se ejecuta en un equipo host que da error

1. Haga una copia de seguridad de los datos importantes de los volúmenes de almacén de instancias en Amazon EBS o en Amazon S3.
2. Detenga la instancia.
3. Inicie la instancia.
4. Restaure los datos importantes.

Para obtener más información, consulte Detención e iniciación de una instancia de Amazon EC2.

Para recuperar una instancia con respaldo en el almacén de instancias que se ejecuta en un equipo host que dio error

1. Cree una AMI a partir de la instancia.
2. Cargue la imagen en Amazon S3.
3. Haga una copia de seguridad de los datos importantes en Amazon EBS o en Amazon S3.
4. Termine la instancia.
5. Lance una instancia nueva desde la AMI.
6. Restaure los datos importantes en la nueva instancia.

Solucionar problemas de detención de la instancia

Si ha detenido la instancia respaldada por Amazon EBS y parece bloqueada en el estado `stopping`, puede deberse a algún problema con el equipo host subyacente.

No tiene costo el uso de la instancia mientras está en el estado `stopping` o en cualquier otro estado excepto `running`. Solo se cobrará por el uso de la instancia cuando su estado sea `running`.

Forzar la detención de la instancia

Fuerce a que la instancia se detenga utilizando la consola o la AWS CLI.

> **Note**
>
> Puede forzar que una instancia deje de usar la consola únicamente mientras la instancia esté en el estado `stopping`. Puede forzar que una instancia deje de usar la AWS CLI mientras la instancia esté en cualquier estado, a excepción de `shutting-down` y `terminated`.

Console

Para forzar la detención de la instancia mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instances (Instancias) y seleccione la instancia bloqueada.
3. Elija Instance state (Estado de instancia), Force stop instance (Forzar detención de instancia), Stop (Detener).

   Tenga en cuenta que Force stop instance (Forzar detención de instancia) solo está disponible en la consola si la instancia tiene el estado `stopping`. Si la instancia tiene otro estado (excepto `shutting-down` y `terminated`), puede utilizar la AWS CLI para forzar la detención de la instancia.

AWS CLI

Para forzar la detención de la instancia mediante el comando AWS CLI

Utilice el comando stop-instances (Detener instancias) y la opción `--force` de la siguiente manera:

```
aws ec2 stop-instances --instance-ids i-0123ab456c789d01e --force
```

Si transcurridos 10 minutos, la instancia no se ha detenido, envíe una solicitud de ayuda en AWS re:Post. Para ayudar a agilizar la solución, incluya el ID de la instancia y describa los pasos que acaba de dar. Si dispone de algún plan de soporte, cree un caso de soporte técnico en el Centro de soporte.

Crear una instancia de sustitución

Para intentar resolver el problema mientras espera ayuda de AWS re:Post o el Centro de soporte, cree una instancia de sustitución. Cree una AMI de la instancia bloqueada y lance una nueva instancia utilizando la nueva AMI.

> **Important**
>
> Se recomienda crear una instancia de sustitución si solo se registran las comprobaciones de estado del sistema, ya que las comprobaciones de estado de instancias harán que la AMI copie una réplica exacta del sistema operativo dañado. Una vez que ha confirmado el mensaje de estado, cree la AMI y lance una nueva instancia con la nueva AMI.

Console

Para crear una instancia de sustitución mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instances (Instancias) y seleccione la instancia bloqueada.
3. Elija Actions (Acciones), Image and templates (Imagen y plantillas), Create image (Crear imagen).
4. En la página Create image (Crear imagen), proceda del siguiente modo:
   a. Escriba un nombre y una descripción de la AMI.
   b. Elija No reboot (Sin reiniciar).
   c. Elija Create image (Crear imagen).

   Para obtener más información, consulte the section called “Creación de una AMI a partir de una instancia”.
5. Lance una nueva instancia desde la AMI y compruebe que funciona.
6. Seleccione la instancia bloqueada y elija Actions (Acciones), Instance state (Estado de la instancia), Terminate instance (Terminar instancia). Si la instancia también se queda bloqueada al terminar, Amazon EC2 fuerza automáticamente la terminación en el plazo de unas horas.

AWS CLI

Para crear una instancia de sustitución mediante la CLI

1. Cree una AMI a partir de la instancia bloqueada utilizando el comando create-image (AWS CLI) y la opción `--no-reboot` como se indica a continuación:

```
aws ec2 create-image --instance-id i-0123ab456c789d01e --name "AMI" --
description "AMI for replacement instance" --no-reboot
```

2. Lance una nueva instancia desde la AMI mediante el comando run-instances (AWS CLI) como se indica a continuación:

```
aws ec2 run-instances --image-id ami-1a2b3c4d --count 1 --instance-type c3.large
 --key-name MyKeyPair --security-groups MySecurityGroup
```

3. Verifique que la nueva instancia está en funcionamiento.
4. Termine la instancia bloqueada utilizando el comando terminate-instances (AWS CLI) como se indica a continuación:

```
aws ec2 terminate-instances --instance-ids i-1234567890abcdef0
```

Si no logra crear una AMI desde la instancia como se ha descrito en el procedimiento previo, puede configurar una instancia de remplazo del modo siguiente:

(Alternativa) Para crear una instancia de sustitución mediante la consola

1. Seleccione la instancia y elija Description (Descripción), Block devices (Dispositivos de bloques). Seleccione cada volumen y anote su ID de volumen. Asegúrese de anotar cuál es el volumen raíz.
2. En el panel de navegación, elija Volumes (Volúmenes). Seleccione cada volumen de la instancia y elija Actions (Acciones), Create Snapshot (Crear instantánea).
3. En el panel de navegación, elija Snapshots (Instantáneas). Seleccione la instantánea que acaba de crear y elija Actions (Acciones), Create Volume (Crear volumen).
4. Lance una instancia con el mismo sistema operativo que la instancia bloqueada. Anote el ID de volumen y el nombre de dispositivo del volumen raíz.

5. En el panel de navegación, elija Instances (Instancias), seleccione la instancia que acaba de lanzar y elija Instance state (Estado de la instancia) y Stop instance (Detener instancia).
6. En el panel de navegación, elija Volumes (Volúmenes), seleccione el volumen raíz de la instancia detenida y elija Actions (Acciones), Detach Volume (Desvincular volumen).
7. Seleccione el volumen raíz que ha creado a partir de la instancia bloqueada, elija Actions (Acciones), Attach Volume (Asociar volumen) y asócielo a la nueva instancia como su volumen raíz (mediante el nombre de dispositivo que anotó). Adjunte cualquier volumen adicional que no sea raíz a la instancia.
8. En el panel de navegación, elija Instances (Instancias) y seleccione la instancia de sustitución. Elija Instance state (Estado de la instancia) y Start instance (Iniciar instancia). Verifique que la instancia está en funcionamiento.
9. Seleccione la instancia bloqueada, elija Instance state (Estado de la instancia) y Terminate instance (Terminar instancia). Si la instancia también se queda bloqueada al terminar, Amazon EC2 fuerza automáticamente la terminación en el plazo de unas horas.

Solucionar problemas de terminación de instancias (cierre)

No se cobra el uso por ninguna instancia hasta que se encuentre en estado `running`. Es decir, cuando termina una instancia, deja de incurrir en gastos en cuanto su estado cambia a `shutting-down`.

La instancia termina inmediatamente

Hay varios problemas pueden hacer que la instancia finalice inmediatamente al iniciarse. Para obtener más información, consulte La instancia termina inmediatamente.

Retrasar la terminación de una instancia

Si la instancia permanece en estado `shutting-down` durante más de unos minutos, puede retrasarse debido a que se están cerrando los scripts que la instancia ejecuta.

Otra causa posible es un problema con el equipo host subyacente. Si la instancia permanece en estado `shutting-down` durante varias horas, Amazon EC2 la trata como si estuviera bloqueada y la termina por la fuerza.

Si parece que la instancia se bloquea al terminar y lleva más de varias horas, envíe una solicitud de ayuda a AWS re:Post. Para ayudar a agilizar la solución, incluya el ID de la instancia y describa los

pasos que acaba de dar. Si dispone de algún plan de soporte, cree un caso de soporte técnico en el Centro de soporte.

Las instancias que han terminado se siguen mostrando

Después de que termine una instancia, permanece visible durante un breve periodo antes de ser eliminada. El estado se muestra como `terminated`. Si la entrada no se elimina transcurridas varias horas, póngase en contacto con Soporte.

Error: es posible que la instancia no se termine. Modifique su atributo de instancia “disableApiTermination”

Si intenta terminar una instancia y aparece el mensaje de error `The instance instance_id may not be terminated. Modify its 'disableApiTermination' instance attribute`, esto indica que la instancia está habilitada para la protección de terminación. La protección de terminación evita que la instancia se termine accidentalmente. Para obtener más información, consulte Cómo habilitar la protección contra la terminación.

Primero debe deshabilitar la protección de terminación antes de terminar la instancia.

Para deshabilitar la protección de terminación mediante la consola de Amazon EC2, seleccione la instancia y, a continuación, elija Acciones, Configuración de la instancia y Cambiar protección de terminación.

Para deshabilitar la protección de terminación con AWS CLI, use el siguiente comando.

```
aws ec2 modify-instance-attribute --instance-id instance_id --no-disable-api-
termination
```

Instancias lanzadas o terminadas automáticamente

En general, los siguientes comportamientos significan que ha utilizado Amazon EC2 Auto Scaling, flota de EC2 o flota de spot para escalar automáticamente los recursos informáticos en función de los criterios que ha definido:

- Se termina una instancia y se lanza automáticamente una nueva instancia.
- Se lanza una instancia y una de las instancias se termina automáticamente.
- Se detiene una instancia y se termina y se lanza automáticamente una nueva instancia.

Para detener el escalado automático, consulte la Guía del usuario de Amazon EC2 Auto Scaling, Flota de EC2 o Creación de una solicitud de flota de spot.

Solución de problemas de las instancias de Linux con comprobaciones de estado no superadas

> **Note**
>
> Este tema se aplica a las instancias de Linux únicamente.

La siguiente información puede ayudarlo a solucionar problemas si la instancia de Linux no supera una comprobación de estado. Determine en primer lugar si las aplicaciones muestran algún problema. Si descubre que la instancia no ejecuta sus aplicaciones según lo previsto, revise la información de comprobación de estado y los registros del sistema.

Para ver ejemplos de problemas que pueden provocar errores en las comprobaciones de estado, consulte Comprobaciones de estado para sus instancias.

Contenido

- fsck: No such file or directory while trying to open... (File system not found)
- General error mounting filesystems (Failed mount) (Error general al montar los sistemas de archivos (no se pudieron montar))
- VFS: Unable to mount root fs on unknown-block (Root filesystem mismatch)
- Error: Unable to determine major/minor number of root device... (Root file system/device mismatch)
- XENBUS: Device with no driver...
- ... days without being checked, check forced (File system check required)
- fsck died with exit status... (Missing device)
- Símbolo de sistema GRUB (grubdom>)
- Bringing up interface eth0: Device eth0 has different MAC address than expected, ignoring. (dirección MAC no modificable)
- Unable to load SELinux Policy. Machine is in enforcing mode. Halting now. (SELinux misconfiguration)
- XENBUS: Timeout connecting to devices (Xenbus timeout)

Revisar información de comprobación de estado

Para investigar las instancias en mal estado con la consola de Amazon EC2

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instances (instancia[s]) y seleccione la instancia.
3. En el panel de detalles, elija Estado y alarmas para ver los resultados individuales de todas las Comprobaciones de estado del sistema y Comprobaciones de estado de instancias.

Si una comprobación de estado del sistema ha dado error, intente con alguna de las opciones siguientes:

- Cree una alarma de recuperación de instancias. Para obtener más información, consulte Crear alarmas que detienen, terminan, reinician o recuperan una instancia.
- Si cambió el tipo de instancia a una instancia integrada en el AWS Nitro System, las comprobaciones de estado fallan si ha migrado desde una instancia que no dispone de los controladores ENA y NVMe necesarios. Para obtener más información, consulte Compatibilidad para cambiar el tipo de instancia.

- Con una instancia que use una AMI respaldada por Amazon EBS, detenga y reinicie la instancia.
- Con una instancia que use una AMI respaldada por un almacén de instancias, termine la instancia y lance una instancia de sustitución.
- Espere a que Amazon EC2 resuelva el problema.
- Publique su problema en AWS re:Post.
- Si la instancia está en un grupo de Auto Scaling, el servicio de Amazon EC2 Auto Scaling inicia automáticamente una instancia de sustitución. Para obtener más información, consulte Comprobaciones de estado de las instancias de Auto Scaling en la Guía del usuario de Amazon EC2 Auto Scaling.
- Recupere el registro del sistema y busque errores.

Recuperación de los registros del sistema

Si la comprobación de estado de la instancia da error, puede reiniciar la instancia y recuperar los registros del sistema. Los registros pueden revelar un error que puede ayudarle a solucionar el problema. La reinicialización elimina la información innecesaria de los registros.

Para reiniciar una instancia y recuperar el registro del sistema

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instances (instancias) y seleccione la instancia.
3. Elija Instance state (Estado de la instancia) y Reboot intance (Reiniciar instancia). Se puede tardar unos minutos en reiniciar la instancia.
4. Verifique que el problema persiste, ya que en algunos casos, el reinicio puede solucionarlo.
5. Cuando la instancia esté en el estado `running`, elija Actions (Acciones), Monitor and troubleshoot (Monitoreo y solución de problemas), Get system log (Obtener registro del sistema).
6. Revise el registro que aparece en la pantalla y use la lista enunciados de errores conocidos del registro del sistema para solventar el problema.
7. Si el problema persiste, puede publicarlo en AWS re:Post.

Solucionar errores del registro del sistema en instancias de Linux

En las instancias de Linux que han dado error en la comprobación de estado, como la prueba accesibilidad de la instancia, compruebe que ha seguido los pasos anteriores para recuperar el

registro del sistema. La lista siguiente incluye algunos errores habituales del sistema y sugiere acciones que se pueden tomar para solucionarlos.

Errores de memoria

- Out of memory: kill process
- ERROR: mmu_update failed (Memory management update failed)

Errores de dispositivo

- Error de E/S (error del dispositivo de bloques)
- I/O ERROR: neither local nor remote disk (Broken distributed block device)

Errores del Kernel

- request_module: runaway loop modprobe (Looping legacy kernel modprobe on older Linux versions)
- "FATAL: kernel too old" and "fsck: No such file or directory while trying to open /dev" (Kernel and AMI mismatch)
- "FATAL: Could not load /lib/modules" o "BusyBox" (Missing kernel modules)
- ERROR Invalid kernel (EC2 incompatible kernel)

Errores del sistema de archivos

- fsck: No such file or directory while trying to open... (File system not found)
- General error mounting filesystems (Failed mount) (Error general al montar los sistemas de archivos (no se pudieron montar))
- VFS: Unable to mount root fs on unknown-block (Root filesystem mismatch)
- Error: Unable to determine major/minor number of root device... (Root file system/device mismatch)
- XENBUS: Device with no driver...
- ... days without being checked, check forced (File system check required)
- fsck died with exit status... (Missing device)

Errores del sistema operativo

- Símbolo de sistema GRUB (grubdom>)
- Bringing up interface eth0: Device eth0 has different MAC address than expected, ignoring. (dirección MAC no modificable)
- Unable to load SELinux Policy. Machine is in enforcing mode. Halting now. (SELinux misconfiguration)
- XENBUS: Timeout connecting to devices (Xenbus timeout)

Out of memory: kill process

Un error de falta de memoria viene indicado en una entrada del registro del sistema similar a la siguiente.

```
[115879.769795] Out of memory: kill process 20273 (httpd) score 1285879
or a child
[115879.769795] Killed process 1917 (php-cgi) vsz:467184kB, anon-
rss:101196kB, file-rss:204kB
```

Causa posible

Memoria agotada

Acciones sugeridas

Para cada tipo de instancia	Haga lo siguiente
Respaldada por Amazon EBS	Aplique alguna de las siguientes acciones: • Detenga la instancia y modifíquela para usar un tipo de instancia diferente, y vuelva a iniciarla. Por ejemplo, un tipo de instancia mayor u optimizada para memoria. • Reinicie la instancia para devolverla a un estado no deteriorado. Es probable que el problema vuelva a producirse a menos que cambie el tipo de instancia.
Con respaldo en el almacén de instancias	Aplique alguna de las siguientes acciones:

Para cada tipo de instancia	Haga lo siguiente
	• Termine la instancia y lance una nueva especificando un tipo de instancia distinto. Por ejemplo, un tipo de instancia mayor u optimizada para memoria. • Reinicie la instancia para devolverla a un estado no deteriorado. Es probable que el problema vuelva a producirse a menos que cambie el tipo de instancia.

ERROR: mmu_update failed (Memory management update failed)

Los errores de actualización de administración de memoria se indican con una entrada de registro similar a la siguiente:

```
...
Press `ESC' to enter the menu... 0   [H[J  Booting 'Amazon Linux 2011.09
 (2.6.35.14-95.38.amzn1.i686)'


root (hd0)

 Filesystem type is ext2fs, using whole disk

kernel /boot/vmlinuz-2.6.35.14-95.38.amzn1.i686 root=LABEL=/ console=hvc0 LANG=

en_US.UTF-8 KEYTABLE=us

initrd /boot/initramfs-2.6.35.14-95.38.amzn1.i686.img

ERROR: mmu_update failed with rc=-22
```

Causa posible

Problema con Amazon Linux

Acción sugerida

Publique el problema en el foro de desarrolladores o contacte con AWS Support.

Error de E/S (error del dispositivo de bloques)

Un error de entrada/salida viene indicado en una entrada del registro del sistema similar al ejemplo siguiente:

```
[9943662.053217] end_request: I/O error, dev sde, sector 52428288
[9943664.191262] end_request: I/O error, dev sde, sector 52428168
[9943664.191285] Buffer I/O error on device md0, logical block 209713024
[9943664.191297] Buffer I/O error on device md0, logical block 209713025
[9943664.191304] Buffer I/O error on device md0, logical block 209713026
[9943664.191310] Buffer I/O error on device md0, logical block 209713027
[9943664.191317] Buffer I/O error on device md0, logical block 209713028
[9943664.191324] Buffer I/O error on device md0, logical block 209713029
[9943664.191332] Buffer I/O error on device md0, logical block 209713030
[9943664.191339] Buffer I/O error on device md0, logical block 209713031
[9943664.191581] end_request: I/O error, dev sde, sector 52428280
[9943664.191590] Buffer I/O error on device md0, logical block 209713136
[9943664.191597] Buffer I/O error on device md0, logical block 209713137
[9943664.191767] end_request: I/O error, dev sde, sector 52428288
[9943664.191970] end_request: I/O error, dev sde, sector 52428288
[9943664.192143] end_request: I/O error, dev sde, sector 52428288
[9943664.192949] end_request: I/O error, dev sde, sector 52428288
[9943664.193112] end_request: I/O error, dev sde, sector 52428288
[9943664.193266] end_request: I/O error, dev sde, sector 52428288
...
```

Causas posibles

Tipo de instancia	Causa posible
Respaldada por Amazon EBS	Un volumen de Amazon EBS con errores
Con respaldo en el almacén de instancias	Una unidad física fallida

Acciones sugeridas

Para cada tipo de instancia	Haga lo siguiente
Respaldada por Amazon EBS	Use el procedimiento siguiente:

Para cada tipo de instancia	Haga lo siguiente
	1. Detenga la instancia. 2. Retire el volumen. 3. Intente recuperar el volumen. **Note** Es una práctica recomendada tomar una instantánea de los volúmenes de Amazon EBS con frecuencia. Esto reduce de manera significativa el riesgo de pérdida de datos como resultado de un error. 4. Vuelva a adjuntar el volumen a la instancia. 5. Inicie la instancia.
Con respaldo en el almacén de instancias	Termine la instancia y lance una nueva. **Note** No se pueden recuperar los datos. Recupere a partir de las copias de seguridad. **Note** Es una práctica recomendada usar Amazon S3 o Amazon EBS para crear copias de seguridad. Los volúmenes con almacén de instancias se vinculan directamente con errores de host único y de disco único.

I/O ERROR: neither local nor remote disk (Broken distributed block device)

Un error de entrada/salida en el dispositivo viene indicado en una entrada del registro del sistema similar al ejemplo siguiente:

```
...
block drbd1: Local IO failed in request_timer_fn. Detaching...

Aborting journal on device drbd1-8.

block drbd1: IO ERROR: neither local nor remote disk

Buffer I/O error on device drbd1, logical block 557056

lost page write due to I/O error on drbd1

JBD2: I/O error detected when updating journal superblock for drbd1-8.
```

Causas posibles

Tipo de instancia	Causa posible
Respaldada por Amazon EBS	Un volumen de Amazon EBS con errores
Con respaldo en el almacén de instancias	Una unidad física fallida

Acción sugerida

Termine la instancia y lance una nueva.

En el caso de una instancia respaldada por Amazon EBS, puede recuperar los datos desde una instantánea reciente creando una imagen de esta. Cualquier dato agregado después de tomar la instantánea no se recuperará.

request_module: runaway loop modprobe (Looping legacy kernel modprobe on older Linux versions)

Este problema viene indicado por una entrada de registro del sistema similar a la siguiente. El uso de un kernel de Linux antiguo o inestable (por ejemplo, 2.6.16-xenU) puede provocar un problema de bucle infinito en el inicio.

```
Linux version 2.6.16-xenU (builder@xenbat.amazonsa) (gcc version 4.0.1
20050727 (Red Hat 4.0.1-5)) #1 SMP Mon May 28 03:41:49 SAST 2007

BIOS-provided physical RAM map:

 Xen: 0000000000000000 - 0000000026700000 (usable)

0MB HIGHMEM available.
...

request_module: runaway loop modprobe binfmt-464c

request_module: runaway loop modprobe binfmt-464c

request_module: runaway loop modprobe binfmt-464c

request_module: runaway loop modprobe binfmt-464c

request_module: runaway loop modprobe binfmt-464c
```

Acciones sugeridas

Para cada tipo de instancia	Haga lo siguiente
Respaldada por Amazon EBS	Use un kernel más reciente, bien basado en GRUB o estático, con una de las opciones siguientes: Opción 1: Termine la instancia y lance una nueva especificando los parámetros `-kernel` y `-ramdisk`. Opción 2:

Para cada tipo de instancia	Haga lo siguiente
	1. Detenga la instancia. 2. Modifique el kernel y los atributos ramdisk para usar el kernel nuevo. 3. Inicie la instancia.
Con respaldo en el almacén de instancias	Termine la instancia y lance una nueva especificando los parámetros `-kernel` y `-ramdisk`.

"FATAL: kernel too old" and "fsck: No such file or directory while trying to open /dev" (Kernel and AMI mismatch)

Este problema viene indicado por una entrada de registro del sistema similar a la siguiente.

```
Linux version 2.6.16.33-xenU (root@dom0-0-50-45-1-a4-ee.z-2.aes0.internal)
(gcc version 4.1.1 20070105 (Red Hat 4.1.1-52)) #2 SMP Wed Aug 15 17:27:36 SAST 2007
...
FATAL: kernel too old
Kernel panic - not syncing: Attempted to kill init!
```

Causas posibles

Kernel y espacio de usuario incompatibles

Acciones sugeridas

Para cada tipo de instancia	Haga lo siguiente
Respaldada por Amazon EBS	Use el procedimiento siguiente: 1. Detenga la instancia. 2. Modifique la configuración para usar un nuevo kernel. 3. Inicie la instancia.
Con respaldo en el almacén de instancias	Use el procedimiento siguiente:

Para cada tipo de instancia	Haga lo siguiente
	1. Cree una AMI que use un kernel más reciente. 2. Termine la instancia. 3. Inicie una nueva instancia desde la AMI que ha creado.

"FATAL: Could not load /lib/modules" o "BusyBox" (Missing kernel modules)

Este problema viene indicado por una entrada de registro del sistema similar a la siguiente.

```
[    0.370415] Freeing unused kernel memory: 1716k freed
Loading, please wait...
WARNING: Couldn't open directory /lib/modules/2.6.34-4-virtual: No such file or
 directory
FATAL: Could not open /lib/modules/2.6.34-4-virtual/modules.dep.temp for writing: No
 such file or directory
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
 directory
Couldn't get a file descriptor referring to the console
Begin: Loading essential drivers... ...
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
 directory
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
 directory
Done.
Begin: Running /scripts/init-premount ...
Done.
Begin: Mounting root file system... ...
Begin: Running /scripts/local-top ...
Done.
Begin: Waiting for root file system... ...
Done.
Gave up waiting for root device.  Common problems:
 - Boot args (cat /proc/cmdline)
   - Check rootdelay= (did the system wait long enough?)
   - Check root= (did the system wait for the right device?)
 - Missing modules (cat /proc/modules; ls /dev)
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
 directory
```

```
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
 directory
ALERT! /dev/sda1 does not exist. Dropping to a shell!


BusyBox v1.13.3 (Ubuntu 1:1.13.3-1ubuntu5) built-in shell (ash)
Enter 'help' for a list of built-in commands.

(initramfs)
```

Causas posibles

Este problema puede deberse a una o varias de las siguientes causas:

- Falta ramdisk
- Faltan los módulos correctos de ramdisk
- El volumen raíz de Amazon EBS no está correctamente adjuntado como `/dev/sda1`

Acciones sugeridas

Para cada tipo de instancia	Haga lo siguiente
Respaldada por Amazon EBS	Use el procedimiento siguiente: 1. Seleccione el ramdisk corregido para el volumen Amazon EBS. 2. Detenga la instancia. 3. Separe el volumen y arréglelo. 4. Adjunte el volumen a la instancia. 5. Inicie la instancia. 6. Modifique la AMI para usar el ramdisk corregido.
Con respaldo en el almacén de instancias	Use el procedimiento siguiente: 1. Termine la instancia y lance una nueva con el ramdisk correcto.

Para cada tipo de instancia	Haga lo siguiente
	2. Cree una nueva AMI con el ramdisk correcto.

ERROR Invalid kernel (EC2 incompatible kernel)

Este problema viene indicado por una entrada de registro del sistema similar a la siguiente.

```
...
root (hd0)

 Filesystem type is ext2fs, using whole disk

kernel /vmlinuz root=/dev/sda1 ro

initrd /initrd.img

ERROR Invalid kernel: elf_xen_note_check: ERROR: Will only load images
built for the generic loader or Linux images
xc_dom_parse_image returned -1

Error 9: Unknown boot failure

  Booting 'Fallback'

root (hd0)

 Filesystem type is ext2fs, using whole disk

kernel /vmlinuz.old root=/dev/sda1 ro

Error 15: File not found
```

Causas posibles

Esto puede deberse a uno o a ambos de los problemas siguientes:

- El kernel proporcionado no es compatible con GRUB
- No existe kernel alternativo

Acciones sugeridas

Para cada tipo de instancia	Haga lo siguiente
Respaldada por Amazon EBS	Use el procedimiento siguiente: 1. Detenga la instancia. 2. Remplácelo con un kernel en funcionam iento. 3. Instale un kernel alternativo. 4. Modifique la AMI corrigiendo el kernel.
Con respaldo en el almacén de instancias	Use el procedimiento siguiente: 1. Termine la instancia y lance una nueva con el kernel correcto. 2. Cree una AMI con el kernel correcto. 3. (Opcional) Busque asistencia técnica para la recuperación de datos a través de AWS Support.

fsck: No such file or directory while trying to open... (File system not found)

Este problema viene indicado por una entrada de registro del sistema similar a la siguiente.

```
  Welcome to Fedora
  Press 'I' to enter interactive startup.
Setting clock : Wed Oct 26 05:52:05 EDT 2011 [  OK  ]

Starting udev: [  OK  ]

Setting hostname localhost:  [  OK  ]

No devices found
Setting up Logical Volume Management: File descriptor 7 left open
  No volume groups found
[  OK  ]
```

```
Checking filesystems
Checking all file systems.
[/sbin/fsck.ext3 (1) -- /] fsck.ext3 -a /dev/sda1
/dev/sda1: clean, 82081/1310720 files, 2141116/2621440 blocks
[/sbin/fsck.ext3 (1) -- /mnt/dbbackups] fsck.ext3 -a /dev/sdh
fsck.ext3: No such file or directory while trying to open /dev/sdh

/dev/sdh:
The superblock could not be read or does not describe a correct ext2
filesystem.  If the device is valid and it really contains an ext2
filesystem (and not swap or ufs or something else), then the superblock
is corrupt, and you might try running e2fsck with an alternate superblock:
    e2fsck -b 8193 <device>

[FAILED]


*** An error occurred during the file system check.
*** Dropping you to a shell; the system will reboot
*** when you leave the shell.
Give root password for maintenance
(or type Control-D to continue):
```

Causas posibles

- Hay un error en las definiciones del sistema de archivos de ramdisk /etc/fstab
- Definiciones del sistema de archivos mal configuradas en /etc/fstab
- Falta la unidad o da error

Acciones sugeridas

Para cada tipo de instancia	Haga lo siguiente
Respaldada por Amazon EBS	Use el procedimiento siguiente: 1. Detenga la instancia, separe el volumen raíz, repare o modifique el volumen, adjunte el volumen a la instancia e inicie la instancia. 2. Corrija ramdisk para incluir /etc/fstab modificado (si procede).

Para cada tipo de instancia	Haga lo siguiente
	3. Modifique la AMI para usar un ramdisk más reciente. El sexto campo de fstab define los requisitos de disponibilidad del montaje: un valor distinto de cero implica que se hará un fsck en dicho volumen y debe ser correcto. El uso de este campo puede ser problemático en Amazon EC2 porque un error genera, por lo general, una pregunta interactiva en la consola que no está disponible actualmente en Amazon EC2. Tenga precaución con esta característica y lea la página de Linux man sobre fstab.
Con respaldo en el almacén de instancias	Use el procedimiento siguiente: 1. Termine la instancia y lance una nueva. 2. Separe los volúmenes errantes de Amazon EBS y reinicie la instancia. 3. (Opcional) Busque asistencia técnica para la recuperación de datos a través de AWS Support.

General error mounting filesystems (Failed mount) (Error general al montar los sistemas de archivos (no se pudieron montar))

Este problema viene indicado por una entrada de registro del sistema similar a la siguiente.

```
Loading xenblk.ko module
xen-vbd: registered block device major 8

Loading ehci-hcd.ko module
Loading ohci-hcd.ko module
Loading uhci-hcd.ko module
USB Universal Host Controller Interface driver v3.0
```

```
Loading mbcache.ko module
Loading jbd.ko module
Loading ext3.ko module
Creating root device.
Mounting root filesystem.
kjournald starting.  Commit interval 5 seconds

EXT3-fs: mounted filesystem with ordered data mode.

Setting up other filesystems.
Setting up new root fs
no fstab.sys, mounting internal defaults
Switching to new root and running init.
unmounting old /dev
unmounting old /proc
unmounting old /sys
mountall:/proc: unable to mount: Device or resource busy
mountall:/proc/self/mountinfo: No such file or directory
mountall: root filesystem isn't mounted
init: mountall main process (221) terminated with status 1

General error mounting filesystems.
A maintenance shell will now be started.
CONTROL-D will terminate this shell and re-try.
Press enter for maintenance
(or type Control-D to continue):
```

Causas posibles

Tipo de instancia	Causa posible
Respaldada por Amazon EBS	• Volumen de Amazon EBS separado o con errores. • Sistema de archivos dañado. • Combinación de ramdisk y AMI errónea (por ejemplo, ramdisk Debian con AMI SUSE).
Con respaldo en el almacén de instancias	• Una unidad fallida.

Tipo de instancia	Causa posible
	• Un sistema de archivos dañado. • Una combinación de ramdisk y AMI errónea (por ejemplo, ramdisk Debian con SUSE AMI).

Acciones sugeridas

Para cada tipo de instancia	Haga lo siguiente
Respaldada por Amazon EBS	Use el procedimiento siguiente: 1. Detenga la instancia. 2. Separe el volumen raíz. 3. Adjunte el volumen raíz a una instancia conocida activa. 4. Ejecute una comprobación del sistema de archivos (fsck –a /dev/...). 5. Corrija los posibles errores. 6. Separe el volumen de la instancia conocida activa. 7. Adjunte el volumen a la instancia detenida. 8. Inicie la instancia. 9. Vuelva a comprobar el estado de la instancia .
Con respaldo en el almacén de instancias	Pruebe con una de las siguientes acciones: • Inicie una nueva instancia. • (Opcional) Busque asistencia técnica para la recuperación de datos a través de AWS Support.

VFS: Unable to mount root fs on unknown-block (Root filesystem mismatch)

Este problema viene indicado por una entrada de registro del sistema similar a la siguiente.

```
Linux version 2.6.16-xenU (builder@xenbat.amazonsa) (gcc version 4.0.1
 20050727 (Red Hat 4.0.1-5)) #1 SMP Mon May 28 03:41:49 SAST 2007
...
Kernel command line:  root=/dev/sda1 ro 4
...
Registering block device major 8
...
Kernel panic - not syncing: VFS: Unable to mount root fs on unknown-block(8,1)
```

Causas posibles

Tipo de instancia	Causa posible
Respaldada por Amazon EBS	• El dispositivo no se ha adjuntado correctamente. • El dispositivo raíz no se ha adjuntado en el punto correcto. • El sistema de archivos no está en el formato esperado. • Se usa un kernel heredado (por ejemplo, 2.6.16-XenU). • Una reciente actualización del kernel en la instancia (actualización con errores o un error de actualización)
Con respaldo en el almacén de instancias	Error del dispositivo de hardware.

Acciones sugeridas

Para cada tipo de instancia	Haga lo siguiente
Respaldada por Amazon EBS	Aplique alguna de las siguientes acciones:

Para cada tipo de instancia	Haga lo siguiente
	• Detenga y vuelva a iniciar la instancia. • Modifique el volumen raíz para adjuntarlo en el punto correcto de dispositivo, /dev/sda1 en lugar de /dev/sda. • Detenga y modifique para usar el kernel moderno. • Consulte la documentación de la distribución de Linux para saber cuáles son los errores de actualización conocidos. Cambie o vuelva a instalar el kernel.
Con respaldo en el almacén de instancias	Termine la instancia y lance una nueva usando con un kernel actual.

Error: Unable to determine major/minor number of root device... (Root file system/device mismatch)

Este problema viene indicado por una entrada de registro del sistema similar a la siguiente.

```
...
XENBUS: Device with no driver: device/vif/0
XENBUS: Device with no driver: device/vbd/2048
drivers/rtc/hctosys.c: unable to open rtc device (rtc0)
Initializing network drop monitor service
Freeing unused kernel memory: 508k freed
:: Starting udevd...
done.
:: Running Hook [udev]
:: Triggering uevents...<30>udevd[65]: starting version 173
done.
Waiting 10 seconds for device /dev/xvda1 ...
Root device '/dev/xvda1' doesn't exist. Attempting to create it.
ERROR: Unable to determine major/minor number of root device '/dev/xvda1'.
You are being dropped to a recovery shell
    Type 'exit' to try and continue booting
sh: can't access tty; job control turned off
```

```
[ramfs /]#
```

Causas posibles

- Falta la unidad de dispositivo de bloques virtual o está incorrectamente configurada
- Discrepancia en la enumeración del dispositivo (sda versus xvda o sda en lugar de sda1)
- Elección incorrecta del kernel de la instancia

Acciones sugeridas

Para cada tipo de instancia	Haga lo siguiente
Respaldada por Amazon EBS	Use el procedimiento siguiente: 1. Detenga la instancia. 2. Retire el volumen. 3. Corrija el problema de mapeo del dispositivo. 4. Inicie la instancia. 5. Modifique la AMI para abordar los problemas de mapeo del dispositivo.
Con respaldo en el almacén de instancias	Use el procedimiento siguiente: 1. Cree una nueva AMI con la corrección (asigne el dispositivo de bloques correctam ente). 2. Termine la instancia y lance una nueva desde la AMI que ha creado.

XENBUS: Device with no driver...

Este problema viene indicado por una entrada de registro del sistema similar a la siguiente.

```
XENBUS: Device with no driver: device/vbd/2048
drivers/rtc/hctosys.c: unable to open rtc device (rtc0)
Initializing network drop monitor service
```

```
Freeing unused kernel memory: 508k freed
:: Starting udevd...
done.
:: Running Hook [udev]
:: Triggering uevents...<30>udevd[65]: starting version 173
done.
Waiting 10 seconds for device /dev/xvda1 ...
Root device '/dev/xvda1' doesn't exist. Attempting to create it.
ERROR: Unable to determine major/minor number of root device '/dev/xvda1'.
You are being dropped to a recovery shell
    Type 'exit' to try and continue booting
sh: can't access tty; job control turned off
[ramfs /]#
```

Causas posibles

- Falta la unidad de dispositivo de bloques virtual o está incorrectamente configurada
- Discrepancia en la enumeración del dispositivo (sda frente a xvda)
- Elección incorrecta del kernel de la instancia

Acciones sugeridas

Para cada tipo de instancia	Haga lo siguiente
Respaldada por Amazon EBS	Use el procedimiento siguiente: 1. Detenga la instancia. 2. Retire el volumen. 3. Corrija el problema de mapeo del dispositivo. 4. Inicie la instancia. 5. Modifique la AMI para abordar los problemas de mapeo del dispositivo.
Con respaldo en el almacén de instancias	Use el procedimiento siguiente: 1. Cree una AMI con la corrección adecuada (asigne el dispositivo de bloques correctam ente).

Para cada tipo de instancia	Haga lo siguiente
	2. Termine la instancia y lance una nueva con la AMI que ha creado.

... days without being checked, check forced (File system check required)

Este problema viene indicado por una entrada de registro del sistema similar a la siguiente.

```
...
Checking filesystems
Checking all file systems.
[/sbin/fsck.ext3 (1) -- /] fsck.ext3 -a /dev/sda1
/dev/sda1 has gone 361 days without being checked, check forced
```

Causas posibles

Terminado el tiempo de comprobación del sistema de archivos; se fuerza una comprobación del sistema de archivos.

Acciones sugeridas

- Espere hasta que finalice la comprobación del sistema de archivos. La comprobación puede llevar mucho tiempo en función del tamaño del sistema de archivos raíz.
- Modifique los sistemas de archivos para quitar el cumplimiento de la comprobación del sistema de archivos (fsck) usando tune2fs o las herramientas adecuadas para el sistema de archivos.

fsck died with exit status... (Missing device)

Este problema viene indicado por una entrada de registro del sistema similar a la siguiente.

```
Cleaning up ifupdown....
Loading kernel modules...done.
...
Activating lvm and md swap...done.
Checking file systems...fsck from util-linux-ng 2.16.2
/sbin/fsck.xfs: /dev/sdh does not exist
fsck died with exit status 8
```

```
[31mfailed (code 8).[39;49m
```

Causas posibles

- Ramdisk busca la unidad que falta
- Forzada la comprobación de la coherencia del sistema de archivos
- Error en la unidad o unidad separada

Acciones sugeridas

Para cada tipo de instancia	Haga lo siguiente
Respaldada por Amazon EBS	Pruebe una o varias de las siguientes opciones para corregir el problema: • Detenga la instancia y adjunte el volumen a una instancia existente en ejecución. • Haga comprobaciones de consistencia manualmente. • Corrija ramdisk para incluir las utilidades relevantes. • Modifique los parámetros de ajuste del sistema de archivos para eliminar los requisitos de consistencia (no se recomiend a).
Con respaldo en el almacén de instancias	Pruebe una o varias de las siguientes opciones para corregir el problema: • Vuelva a empaquetar ramdisk con las herramientas correctas. • Modifique los parámetros de ajuste del sistema de archivos para eliminar los requisitos de consistencia (no se recomiend a). • Termine la instancia y lance una nueva.

Para cada tipo de instancia	Haga lo siguiente
	• (Opcional) Busque asistencia técnica para la recuperación de datos a través de AWS Support.

Símbolo de sistema GRUB (grubdom>)

Este problema viene indicado por una entrada de registro del sistema similar a la siguiente.

```
    GNU GRUB  version 0.97  (629760K lower / 0K upper memory)

       [ Minimal BASH-like line editing is supported.   For

         the   first   word,  TAB  lists  possible  command

         completions.  Anywhere else TAB lists the possible

         completions of a device/filename. ]

grubdom>
```

Causas posibles

Tipo de instancia	Causas posibles
Respaldada por Amazon EBS	• Falta el archivo de configuración de GRUB. • Se ha usado la imagen de GRUB incorrecta, se espera el archivo de configuración de GRUB en una ubicación diferente. • Se ha utilizado un sistema de archivos no compatible para almacenar el archivo de configuración de GRUB (por ejemplo, convertir el sistema de archivos raíz en un tipo que no es compatible con una versión anterior de GRUB).
Con respaldo en el almacén de instancias	• Falta el archivo de configuración de GRUB.

Tipo de instancia	Causas posibles
	• Se ha usado la imagen de GRUB incorrecta, se espera el archivo de configuración de GRUB en una ubicación diferente. • Se ha utilizado un sistema de archivos no compatible para almacenar el archivo de configuración de GRUB (por ejemplo, convertir el sistema de archivos raíz en un tipo que no es compatible con una versión anterior de GRUB).

Acciones sugeridas

Para cada tipo de instancia	Haga lo siguiente
Respaldada por Amazon EBS	Opción 1: Modifique la AMI y vuelva a iniciar la instancia: 1. Modifique la AMI de origen para crear un archivo de configuración de GRUB en la ubicación estándar (/boot/grub/menu.lst). 2. Verifique que la versión de GRUB admite el tipo de sistema de archivos subyacente y actualice GRUB si es necesario. 3. Elija la imagen de GRUB adecuada, (unidad hd0-1st o unidad hd00 – 1st, 1ª partición). 4. Termine la instancia y lance una nueva con la AMI que ha creado. Opción 2: Corrija la instancia existente: 1. Detenga la instancia. 2. Separe el sistema de archivos raíz.

Para cada tipo de instancia	Haga lo siguiente
	3. Adjunte el sistema de archivos raíz a una instancia conocida activa. 4. Monte el sistema de archivos. 5. Cree un archivo de configuración de GRUB. 6. Verifique que la versión de GRUB admite el tipo de sistema de archivos subyacente y actualice GRUB si es necesario. 7. Separe el sistema de archivos. 8. Adjúntelo a la instancia original. 9. Modifique el atributo de kernel para usar la imagen de GRUB adecuada (1er disco o 1ª partición del 1er disco). 10. Inicie la instancia.

Para cada tipo de instancia	Haga lo siguiente
Con respaldo en el almacén de instancias	Opción 1: Modifique la AMI y vuelva a iniciar la instancia: 1. Cree la nueva AMI con un archivo de configuración de GRUB en la ubicación estándar (/boot/grub/menu.lst). 2. Elija la imagen de GRUB adecuada, (unidad hd0-1st o unidad hd00 – 1st, 1ª partición). 3. Verifique que la versión de GRUB admite el tipo de sistema de archivos subyacente y actualice GRUB si es necesario. 4. Termine la instancia y lance una nueva con la AMI que ha creado. Opción 2: Termine la instancia y lance una nueva especificando el kernel correcto. **Note** Para recuperar los datos de la instancia existente, contáctese con AWS Support.

Bringing up interface eth0: Device eth0 has different MAC address than expected, ignoring. (dirección MAC no modificable)

Este problema viene indicado por una entrada de registro del sistema similar a la siguiente.

```
...
Bringing up loopback interface:  [  OK  ]

Bringing up interface eth0:  Device eth0 has different MAC address than expected,
 ignoring.
[FAILED]
```

```
Starting auditd: [  OK  ]
```

Causas posibles

Hay una MAC de interfaz codificada de forma rígida en la configuración de la AMI.

Acciones sugeridas

Para cada tipo de instancia	Haga lo siguiente
Respaldada por Amazon EBS	Aplique alguna de las siguientes acciones: • Modifique la AMI para quitar la codificación rígida y vuelva a iniciar la instancia. • Modifique la instancia para quitar la dirección MAC codificada de forma rígida. O BIEN Use el procedimiento siguiente: 1. Detenga la instancia. 2. Separe el volumen raíz. 3. Adjunte el volumen a otra instancia y modifique el volumen para quitar la dirección MAC codificada de forma rígida. 4. Adjunte el volumen a la instancia original. 5. Inicie la instancia.
Con respaldo en el almacén de instancias	Aplique alguna de las siguientes acciones: • Modifique la instancia para quitar la dirección MAC codificada de forma rígida. • Termine la instancia y lance una nueva.

Unable to load SELinux Policy. Machine is in enforcing mode. Halting now. (SELinux misconfiguration)

Este problema viene indicado por una entrada de registro del sistema similar a la siguiente.

```
audit(1313445102.626:2): enforcing=1 old_enforcing=0 auid=4294967295
Unable to load SELinux Policy. Machine is in enforcing mode. Halting now.
Kernel panic - not syncing: Attempted to kill init!
```

Causas posibles

SELinux se ha habilitado con error:

- El kernel proporcionado no es compatible con GRUB
- No existe kernel alternativo

Acciones sugeridas

Para cada tipo de instancia	Haga lo siguiente
Respaldada por Amazon EBS	Use el procedimiento siguiente: 1. Detenga la instancia fallida. 2. Separe el volumen raíz de la instancia fallida. 3. Adjunte el volumen raíz a otra instancia en ejecución de Linux (referida posteriormente como una instancia de recuperación). 4. Conéctese a la instancia de recuperación y monte el volumen raíz en la instancia fallida. 5. Deshabilite SELinux en el volumen raíz montado. Este proceso varía entre las distribuciones de Linux; para obtener más información, consulte la documentación específica del sistema operativo.

Para cada tipo de instancia	Haga lo siguiente
	Note En algunos sistemas, SELinux se deshabilita estableciendo `SELINUX=disabled` en el archivo `/mount_point /etc/sysconfig/selinux`, donde *mount_point* es la ubicación de la instancia de recuperación en la que montó el volumen. 6. Desmonte y separe el volumen raíz de la instancia de recuperación y vuelva a adjuntarlo a la instancia original. 7. Inicie la instancia.
Con respaldo en el almacén de instancias	Use el procedimiento siguiente: 1. Termine la instancia y lance una nueva. 2. (Opcional) Busque asistencia técnica para la recuperación de datos a través de AWS Support.

XENBUS: Timeout connecting to devices (Xenbus timeout)

Este problema viene indicado por una entrada de registro del sistema similar a la siguiente.

```
Linux version 2.6.16-xenU (builder@xenbat.amazonsa) (gcc version 4.0.1
20050727 (Red Hat 4.0.1-5)) #1 SMP Mon May 28 03:41:49 SAST 2007
...
XENBUS: Timeout connecting to devices!
...
Kernel panic - not syncing: No init found.  Try passing init= option to kernel.
```

Causas posibles

- El dispositivo de bloques no está conectado a la instancia
- Esta instancia usa un kernel de instancias antiguo

Acciones sugeridas

Para cada tipo de instancia	Haga lo siguiente
Respaldada por Amazon EBS	Aplique alguna de las siguientes acciones: • Modifique la AMI y la instancia para usar un kernel moderno y volver a iniciar la instancia. • Reinicie la instancia.
Con respaldo en el almacén de instancias	Aplique alguna de las siguientes acciones: • Termine la instancia. • Modifique la AMI para usar un kernel moderno y lance una nueva instancia usando con esta AMI.

Solucione los problemas de arranque de una instancia de Linux desde un volumen incorrecto

> **Note**
>
> Este tema de solución de problemas se aplica únicamente a las instancias de Linux.

En algunas situaciones, puede suceder que un volumen que no es el volumen adjunto a `/dev/xvda` o `/dev/sda` se ha convertido en el volumen raíz de la instancia. Esto puede suceder cuando se ha adjuntado el volumen raíz de otra instancia o un volumen creado a partir de una instantánea de un volumen raíz, a una instancia que ya tiene un volumen raíz.

Esto sucede por el funcionamiento de ramdisk inicial en Linux. Elige el volumen definido como `/` en `/etc/fstab` y, en algunas distribuciones, esto lo determina la etiqueta adjuntada a la partición del volumen. En concreto, `/etc/fstab` tiene un aspecto como el siguiente:

```
LABEL=/ / ext4 defaults,noatime 1 1
tmpfs /dev/shm tmpfs defaults 0 0
devpts /dev/pts devpts gid=5,mode=620 0 0
sysfs /sys sysfs defaults 0 0
proc /proc proc defaults 0 0
```

Si comprobara las etiquetas de ambos volúmenes, vería que ambos contienen la etiqueta `/`:

```
[ec2-user ~]$ sudo e2label /dev/xvda1
/
[ec2-user ~]$ sudo e2label /dev/xvdf1
/
```

En este ejemplo, acabaría con `/dev/xvdf1` convirtiéndose en el dispositivo raíz en que la instancia se inicia después de ejecutar ramdisk inicial, en lugar del volumen `/dev/xvda1` desde el que pretendía iniciarla. Para resolverlo, utilice el mismo comando e2label para cambiar la etiqueta del volumen adjunto desde el que no quiere arrancar.

En algunos casos, se resuelve si especifica un UUID en `/etc/fstab`. Sin embargo, si ambos volúmenes proceden de la misma instantánea o si el secundario se crea a partir de una instantánea del volumen principal, ambos comparten el UUID.

```
[ec2-user ~]$ sudo blkid
/dev/xvda1: LABEL="/" UUID=73947a77-ddbe-4dc7-bd8f-3fe0bc840778 TYPE="ext4"
 PARTLABEL="Linux" PARTUUID=d55925ee-72c8-41e7-b514-7084e28f7334
/dev/xvdf1: LABEL="old/" UUID=73947a77-ddbe-4dc7-bd8f-3fe0bc840778 TYPE="ext4"
 PARTLABEL="Linux" PARTUUID=d55925ee-72c8-41e7-b514-7084e28f7334
```

Para cambiar la etiqueta de un volumen ext4 adjunto

1. Utilice el comando e2label para cambiar la etiqueta del volumen por algo distinto de `/`.

   ```
   [ec2-user ~]$ sudo e2label /dev/xvdf1 old/
   ```

2. Verifique que el volumen tiene la nueva etiqueta

```
[ec2-user ~]$ sudo e2label /dev/xvdf1
old/
```

Para cambiar la etiqueta de un volumen xfs adjunto

- Utilice el comando xfs_admin para cambiar la etiqueta del volumen por algo distinto de /.

```
[ec2-user ~]$ sudo xfs_admin -L old/ /dev/xvdf1
writing all SBs
new label = "old/"
```

Después de cambiar la etiqueta del volumen de la forma indicada, debería poder reiniciar la instancia y conseguir que el ramdisk inicial seleccione el volumen correcto cuando la instancia se inicia.

> **Important**
>
> Si pretende separar el volumen con la nueva etiqueta y devolverlo a otra instancia para que se use como volumen raíz, debe repetir el procedimiento anterior y cambiar la etiqueta del volumen a su valor original. Si no, la otra instancia no arranca porque ramdisk no encuentra el volumen con la etiqueta /.

Solución de problemas de Sysprep con instancias de Windows

> **Note**
>
> Este tema de solución de problemas se aplica únicamente a las instancias de Windows.

Si tiene problemas o recibe mensajes de error durante la preparación de la imagen, revise los siguientes registros. La ubicación del registro varía en función de si se está ejecutando EC2Config, EC2Launch v1 o EC2Launch v2 con Sysprep.

- `%WINDIR%\Panther\Unattendgc` (EC2Config, EC2Launch v1 y EC2Launch v2)
- `%WINDIR%\System32\Sysprep\Panther` (EC2Config, EC2Launch v1 y EC2Launch v2)

- `C:\Program Files\Amazon\Ec2ConfigService\Logs\Ec2ConfigLog.txt` (únicamente EC2Config)
- `C:\ProgramData\Amazon\Ec2Config\Logs` (únicamente EC2Config)
- `C:\ProgramData\Amazon\EC2-Windows\Launch\Log\EC2Launch.log` (únicamente EC2Launch v1)
- `%ProgramData%\Amazon\EC2Launch\log\agent.log` (únicamente EC2Launch v2)

Si recibe un mensaje de error durante la preparación de la imagen con Sysprep, el sistema operativo podría no estar disponible. Para revisar los archivos de registro, debe parar la instancia, adjuntar su volumen a otra instancia en buen estado como volumen secundario y, a continuación, revisar los registros mencionados en dicho volumen secundario. Para obtener más información acerca del propósito de los archivos de registro por nombre, consulte Archivos de registro relacionados con la instalación de Windows en la documentación de Microsoft.

Si encuentra errores en el archivo de registro Unattendgc, utilice Microsoft Error Lookup Tool para obtener más detalles sobre el error. El siguiente error notificado en el archivo de registro Unattendgc suele deberse a la existencia de uno o varios perfiles de usuario dañados en la instancia:

```
Error [Shell Unattend] _FindLatestProfile failed (0x80070003) [gle=0x00000003]
Error [Shell Unattend] CopyProfile failed (0x80070003) [gle=0x00000003]
```

Existen dos opciones para resolver este problema:

Opción 1

Utilice Regedit en la instancia para buscar la siguiente clave. Verifique que no existen claves de registro de perfil para un usuario eliminado.

`[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\`

Opción 2

1. Modifique el archivo relevante como se indica a continuación:

   - Windows Server 2012 R2 y versiones anteriores: modifique el archivo de respuesta de EC2Config (`C:\Program Files\Amazon\Ec2ConfigService\sysprep2008.xml`).
   - Windows Server 2016 y 2019: edite el archivo de respuesta unattend.xml (`C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep\Unattend.xml`).

- Windows Server 2022: edite el archivo de respuesta unattend.xml (`C:\ProgramData\Amazon\EC2Launch\sysprep\unattend.xml`).

2. Cambie `<CopyProfile>true</CopyProfile>` a `<CopyProfile>false</CopyProfile>`.
3. Vuelva a ejecutar Sysprep. Tenga en cuenta que este cambio de configuración eliminará el perfil de usuario administrador integrado una vez se complete Sysprep.

Usar EC2Rescue para Linux

EC2Rescue para Linux es una herramienta de código abierto fácil de utilizar que se puede ejecutar en una instancia de Linux de Amazon EC2 para diagnosticar y solucionar problema comunes utilizando su biblioteca de más de 100 módulos. Unos pocos casos de uso generalizados para EC2Rescue para Linux incluyen la recopilación de logs de administrador de paquetes y syslog, recopilación de datos de utilización de recursos y diagnóstico/corrección de parámetros de kernel problemáticos conocidos y problemas comunes de OpenSSH.

El runbook de `AWSSupport-TroubleshootSSH` instala EC2Rescue para Linux y luego usa la herramienta para comprobar o intentar solucionar problemas comunes que impiden una conexión remota a un equipo Linux a través de SSH. Para obtener más información y para ejecutar esta automatización, consulte AWS Support-TroubleshootSSH.

Si usa una instancia de Windows, consulte the section called “EC2Rescue for Windows Server”.

Contenido

Instalar EC2Rescue para Linux

La herramienta EC2Rescue para Linux se puede instalar en una instancia de Linux Amazon EC2 que responda a los prerrequisitos siguientes.

Requisitos previos

- Sistemas operativos compatibles:

  - Amazon Linux 2
  - Amazon Linux 2016.09+
  - SUSE Linux Enterprise Server 12+
  - RHEL 7+
  - Ubuntu 16.04+
- Requisitos de software:
  - Python 2.7.9+ o 3.2+

El runbook de `AWSSupport-TroubleshootSSH` instala EC2Rescue para Linux y luego usa la herramienta para comprobar o intentar solucionar problemas comunes que impiden una conexión remota a un equipo Linux a través de SSH. Para obtener más información y para ejecutar esta automatización, consulte AWS Support-TroubleshootSSH.

Si su sistema tiene la versión de Python necesaria, puede instalar la compilación estándar. De lo contrario, puede instalar la compilación incluida, la cual lleva una copia mínima de Python.

Para instalar la compilación estándar

1. En una instancia de Linux en ejecución, descargue la herramienta EC2Rescue para Linux:

   ```
   curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.tgz
   ```

2. (Opcional) Antes de continuar, si lo desea, puede verificar la firma del archivo de instalación de EC2Rescue para Linux. Para obtener más información, consulte (Opcional) Verificar la firma de EC2Rescue para Linux.
3. Descargue el archivo hash sha256:

   ```
   curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.tgz.sha256
   ```

4. Compruebe la integridad del archivo tarball:

   ```
   sha256sum -c ec2rl.tgz.sha256
   ```

5. Descomprima el archivo tarball:

   ```
   tar -xzvf ec2rl.tgz
   ```

6. Verifique la instalación enumerando el archivo de ayuda:

```
cd ec2rl-<version_number>
./ec2rl help
```

Para instalar la compilación incluida

Para ver un enlace a la descarga y la lista de limitaciones, consulte EC2Rescue para Linux en github.

(Opcional) Verificar la firma de EC2Rescue para Linux

A continuación se detalla el proceso recomendado para verificar la validez del paquete de EC2Rescue para Linux para los sistemas operativos basados en Linux.

Siempre que descargue una aplicación de Internet, le recomendamos que compruebe la identidad del editor del software y verifique que la aplicación no ha sido alterada ni se ha visto corrompida desde que se publicó. Esto le protege ante una posible instalación de una versión de la aplicación que contenga un virus u otro código malintencionado.

Si después de seguir los pasos descritos en este tema determina que el software del agente de EC2Rescue para Linux ha sido modificado o está dañado, no ejecute el archivo de instalación. En lugar de hacerlo, póngase en contacto con Amazon Web Services.

Los archivos de EC2Rescue para Linux para los sistemas operativos basados en Linux se firman con GnuPG, una implementación de código abierto del estándar Pretty Good Privacy (OpenPGP) para firmas digitales seguras. GnuPG (también conocido como GPG) permite realizar la autenticación y verificar la integridad mediante el uso de una firma digital. AWS publica una clave pública y firmas que pueden utilizarse para comprobar el paquete de EC2Rescue para Linux descargado. Para obtener más información sobre PGP y GnuPG (GPG), consulte http://www.gnupg.org.

El primer paso consiste en establecer una relación de confianza con el editor del software. Descargue la clave pública del editor de software, compruebe que el propietario de la clave pública es quien afirma ser y, a continuación, agregue la clave pública a su llavero. Su llavero es una colección de claves públicas conocidas. Tras establecer la autenticidad de la clave pública, puede usarla para verificar la firma de la aplicación.

Tareas

- Instalar las herramientas de GPG
- Autenticar e importar la clave pública
- Verificar la firma del paquete

Instalar las herramientas de GPG

Si su sistema operativo es Linux o Unix, es posible que las herramientas de GPG ya estén instaladas. Para comprobar si las herramientas están instaladas en el sistema, escriba gpg2 en un símbolo del sistema. Si las herramientas de GPG están instaladas, verá un símbolo del sistema de GPG. Si las herramientas de GPG no están instaladas, verá un error que afirma que no se puede encontrar el comando. Puede instalar el paquete GnuPG desde un repositorio.

Para instalar las herramientas de GPG en Linux basado en Debian

- En un terminal, ejecute el comando siguiente:

```
apt-get install gnupg2
```

Para instalar las herramientas GPG en Linux basado en Red Hat

- En un terminal, ejecute el comando siguiente:

```
yum install gnupg2
```

Autenticar e importar la clave pública

El siguiente paso del proceso consiste en autenticar la clave pública de EC2Rescue para Linux y agregarla como una clave de confianza al llavero de GPG.

Para autenticar e importar la clave pública de EC2Rescue para Linux

1. En un símbolo del sistema, utilice el comando siguiente para obtener una copia de la clave de compilación pública de GPG:

   ```
   curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.key
   ```

2. En un símbolo del sistema, en el directorio donde haya guardado `ec2rl.key`, use el siguiente comando para importar la clave pública de EC2Rescue para Linux en su llavero:

   ```
   gpg2 --import ec2rl.key
   ```

   El comando devuelve resultados similares a los siguientes:

```
gpg: /home/ec2-user/.gnupg/trustdb.gpg: trustdb created
gpg: key 2FAE2A1C: public key "ec2autodiag@amazon.com <EC2 Rescue for Linux>"
 imported
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)
```

Verificar la firma del paquete

Después de haber instalado las herramientas de GPG, haber autenticado e importado la clave pública de EC2Rescue para Linux y haber comprobado que la clave pública de EC2Rescue para Linux es de confianza, estará listo para verificar la firma del script de instalación de EC2Rescue para Linux.

Para verificar la firma del script de instalación de EC2Rescue para Linux

1. En el símbolo del sistema, ejecute el siguiente comando para descargar el archivo de firma para el script de instalación:

   ```
   curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.tgz.sig
   ```

2. Verifique la firma utilizando un símbolo del sistema para ejecutar el siguiente comando en el directorio donde haya guardado `ec2rl.tgz.sig` y el archivo de instalación de EC2Rescue para Linux. Ambos archivos deben estar presentes.

   ```
   gpg2 --verify ./ec2rl.tgz.sig
   ```

   El resultado debería tener un aspecto similar al siguiente:

   ```
   gpg: Signature made Thu 12 Jul 2018 01:57:51 AM UTC using RSA key ID 6991ED45
   gpg: Good signature from "ec2autodiag@amazon.com <EC2 Rescue for Linux>"
   gpg: WARNING: This key is not certified with a trusted signature!
   gpg:          There is no indication that the signature belongs to the owner.
   Primary key fingerprint: E528 BCC9 0DBF 5AFA 0F6C  C36A F780 4843 2FAE 2A1C
        Subkey fingerprint: 966B 0D27 85E9 AEEC 1146  7A9D 8851 1153 6991 ED45
   ```

   Si el resultado contiene la expresión `Good signature from "ec2autodiag@amazon.com <EC2 Rescue for Linux>"`, significa que la firma se ha verificado correctamente y que se puede ejecutar el script de instalación de EC2Rescue para Linux.

Si el resultado incluye la expresión `BAD signature`, compruebe si ha realizado el procedimiento correctamente. Si sigue recibiendo esta respuesta, póngase en contacto con Amazon Web Services y no ejecute el archivo de instalación descargado anteriormente.

A continuación, se describen en detalle las advertencias que podría recibir:

- WARNING: This key is not certified with a trusted signature! There is no indication that the signature belongs to the owner. Esto afecta a su nivel personal de confianza, ya que no puede tener la certeza de que posee una clave pública auténtica para EC2Rescue para Linux. En un mundo ideal, visitaría una oficina de Amazon Web Services y recibiría la clave en persona. Sin embargo, lo habitual es que la descargue desde un sitio web. En este caso, el sitio web pertenece a Amazon Web Services.
- gpg2: no ultimately trusted keys found. Esto significa que la clave específica no es "definitivamente fiable" para usted (o para otras personas en las que usted confía).

Para obtener más información, consulte http://www.gnupg.org.

Trabajar con EC2Rescue para Linux

A continuación se muestran algunas tareas comunes que puede realizar para comenzar a usar esta herramienta.

Tareas

- Ejecute EC2Rescue para Linux
- Cargar los resultados
- Crear copias de seguridad
- Obtención de ayuda

Ejecute EC2Rescue para Linux

Puede ejecutar EC2Rescue para Linux como se muestra en los siguientes ejemplos.

Example Ejemplo: Ejecutar todos los módulos

Para ejecutar todos los módulos, ejecute EC2Rescue para Linux sin indicar ninguna opción:

```
./ec2rl run
```

Algunos módulos requieren acceso raíz. Si no es usuario raíz, utilice sudo para ejecutar estos módulos como se indica a continuación:

```
sudo ./ec2rl run
```

Example Ejemplo: Ejecutar un módulo específico

para ejecutar solo módulos específicos, utilice el parámetro --only-modules:

```
./ec2rl run --only-modules=module_name --arguments
```

Por ejemplo, este comando ejecuta el módulo dig para enviar consultas al dominio `amazon.com`:

```
./ec2rl run --only-modules=dig --domain=amazon.com
```

Example Ejemplo: Ver los resultados

Puede ver los resultados en `/var/tmp/ec2rl`:

```
cat /var/tmp/ec2rl/logfile_location
```

Por ejemplo, para ver el archivo de registro del módulo dig:

```
cat /var/tmp/ec2rl/2017-05-11T15_39_21.893145/mod_out/run/dig.log
```

Cargar los resultados

Si AWS Support ha solicitado los resultados o compartir los resultados de un bucket de S3, cárguelos con la herramienta de la CLI de EC2Rescue para Linux. El resultado de los comandos EC2Rescue para Linux deberían proporcionar los comandos que necesita utilizar.

Example Ejemplo: Cargar resultados a AWS Support

```
./ec2rl upload --upload-directory=/var/tmp/ec2rl/2017-05-11T15_39_21.893145 --support-url="URLProvidedByAWSSupport"
```

Example Ejemplo: Cargar los resultados en un bucket de S3

```
./ec2rl upload --upload-directory=/var/tmp/ec2rl/2017-05-11T15_39_21.893145 --
presigned-url="YourPresignedS3URL"
```

Para obtener más información acerca de cómo generar URL prefirmadas para Amazon S3, consulte Carga de objetos con direcciones URL prefirmadas.

Crear copias de seguridad

Cree una copia de seguridad de la instancia, uno o varios volúmenes o un ID de dispositivo específico con los comandos siguientes.

Example Ejemplo: Hacer una copia de seguridad de una instancia con una imagen de Amazon Machine (AMI)

```
./ec2rl run --backup=ami
```

Example Ejemplo: Crear una copia de seguridad de todos los volúmenes asociados con la instancia

```
./ec2rl run --backup=allvolumes
```

Example Ejemplo: Hacer una copia de seguridad de un volumen específico

```
./ec2rl run --backup=volumeID
```

Obtención de ayuda

EC2Rescue para Linux incluye un archivo de ayuda en el que se ofrece información y sintaxis de cada comando disponible.

Example Ejemplo: Mostrar la ayuda general

```
./ec2rl help
```

Example Ejemplo: Ver una lista con los módulos disponibles

```
./ec2rl list
```

Example Ejemplo: Mostrar la ayuda para un módulo específico

```
./ec2rl help module_name
```

Por ejemplo, use el siguiente comando para mostrar el archivo de ayuda para el módulo dig:

```
./ec2rl help dig
```

Desarrollar módulos EC2Rescue

Los módulos se escriben en YAML, un estándar de serialización de datos. Un archivo YAML de un módulo consta de un único documento que representa el módulo y sus atributos.

Agregar atributos de módulo

En la tabla siguiente se muestran los atributos de módulo disponibles.

Atributo	Descripción
name (nombre)	Nombre del módulo. El nombre debe tener 18 caracteres o menos de longitud.
version	Número de versión del módulo.
title	Un título breve y descriptivo para el módulo. Este valor debe tener 50 caracteres o menos de longitud.

helptext	La descripción ampliada del módulo. Cada línea debe tener 75 caracteres o menos de longitud. Si el módulo consume argumentos, requeridos y opcionales, inclúyalos en el valor de helptext.
	
	Por ejemplo:
	
	`helptext: !!str |`
	`  Collect output from ps for system analysis`

Atributo	Descripción
	`Consumes --times= for number of times to repeat` `Consumes --period= for time period between repetition`
placement	La fase en la que debe ejecutarse el módulo. Valores admitidos: • prediagnostic • run • postdiagnostic
language	El lenguaje en que está escrito el código del módulo. Valores admitidos: • bash • python **Note** El código Python debe ser compatible con Python 2.7.9+ y Python 3.2+.
remediation	Indica si el módulo admite remedio. Los valores admitidos son `True` o `False`. El módulo tomará el valor predeterminado `False` si está ausente, lo que lo convertirá en un atributo opcional para los módulos que no admiten el remedio.
content	La totalidad del código de script.
constraint	El nombre del objeto que contiene los valores de restricción.

Atributo	Descripción
dominio	Un descriptor del modo en que el módulo se agrupa o clasifica. El conjunto de módulos incluidos usa los dominios siguientes: • revisiones de • net • os • performance
class	Un descriptor del tipo de tarea que realiza el módulo. El conjunto de módulos incluidos usa las clases siguientes: • collect (recopila el resultado de los programas) • diagnose (pase/error según un grupo de criterios) • gather (copia archivos y escribe en un archivo específico)
distro	La lista de distribuciones Linux que admite este módulo. El conjunto de módulos incluidos usa las distribuciones siguientes: • alami (Amazon Linux) • rhel • ubuntu • suse
obligatorio	Los argumentos requeridos que el módulo usa para las opciones de la CLI.
opcional	Los argumentos opcionales que el módulo puede usar.

Atributo	Descripción
software	Los ejecutables de software usados en el módulo. Este atributo tiene como finalidad especificar software que no está instalado de manera predeterminada. La lógica de EC2Rescue para Linux asegura que estos programas sean ejecutables y estén presentes antes de ejecutar el módulo.
package	El paquete de software de origen para un ejecutable. Este atributo tiene como finalidad proporcionar detalles ampliados sobre el paquete con el software, incluida una URL para descargar u obtener más información.
sudo	Indica si se requiere acceso raíz para ejecutar el módulo. No necesita implementar las comprobaciones sudo en el script del módulo. Si el valor es verdadero, la lógica de EC2Rescue para Linux solo ejecuta el módulo cuando el usuario ejecutante tiene acceso raíz.
perfimpact	Indica si el módulo puede tener un impacto significativo de desempeño en el entorno en que se ejecuta. Si el valor es verdadero y el argumento `--perfimpact=true` no está presente, el módulo se omite.
parallelexclusive	Especifica un programa que requiere exclusividad mutua. Por ejemplo, todos los módulos que especifican "bpf" se ejecutan en serie.

Agregar variables de entorno

En la tabla siguiente se muestran las variables de entorno disponibles.

Variable de entorno	Descripción
EC2RL_CALLPATH	La ruta a `ec2rl.py`. Esta ruta se puede usar para ubicar el directorio lib y usar los módulos de Python proporcionados.
EC2RL_WORKDIR	El directorio tmp principal de la herramienta de diagnóstico. Valor predeterminado: `/var/tmp/ec2rl` .
EC2RL_RUNDIR	El directorio donde se almacenan todos los resultados. Valor predeterminado: `/var/tmp/ec2rl/<date&timestamp>` .
EC2RL_GATHEREDDIR	El directorio raíz donde se colocan los datos recopilados del módulo. Valor predeterminado:`/var/tmp/ec2rl/<date&timestamp>/mod_out/gathered/` .
EC2RL_NET_DRIVER	El controlador en uso para la primera interfaz de red no virtual en orden alfabético en la instancia. Ejemplos: • xen_netfront • ixgbevf • ena
EC2RL_SUDO	Es verdadero si EC2Rescue para Linux se ejecuta como raíz; de lo contrario, es falso.
EC2RL_VIRT_TYPE	El tipo de virtualización según lo proporcionan los metadatos de la instancia.

Variable de entorno	Descripción
	Ejemplos: • default-hvm • default-paravirtual
`EC2RL_INTERFACES`	Una lista numerada de interfaces en el sistema. El valor es una cadena que contiene nombres como `eth0`, `eth1`, etcétera. Se genera mediante `functions.bash` y solo está disponible para los módulos de los que se obtiene.

Usar sintaxis YAML

Cuando se construyen los archivos YAML de un módulo, se debe tener en cuenta lo siguiente:

- Tres guiones (`---`) denotan el inicio explícito de un documento.
- La etiqueta `!ec2rlcore.module.Module` dice al analizador YAML a qué constructor llamar cuando se crea el objeto del flujo de datos. Encontrará el constructor dentro del archivo `module.py`.
- La etiqueta `!!str` indica al analizador YAML que no intente determinar el tipo de datos y que interprete el contenido como un literal de cadena.
- El carácter `|` indica al analizador YAML que el valor es un escalar de estilo literal. En este caso, el analizador incluye todos los espacios en blanco. Esto es importante para los módulos porque se mantienen la sangría y los caracteres de nueva línea.
- La sangría estándar de YAML son dos espacios, como se puede ver en los ejemplos siguientes. Asegúrese de que mantiene la sangría estándar (por ejemplo, cuatro espacios para Python) para el script y después sangría de dos espacios para todo el contenido en el archivo del módulo.

Módulos de ejemplo

Ejemplo uno (`mod.d/ps.yaml`):

```
--- !ec2rlcore.module.Module
# Module document. Translates directly into an almost-complete Module object
```

```
name: !!str ps
path: !!str
version: !!str 1.0
title: !!str Collect output from ps for system analysis
helptext: !!str |
  Collect output from ps for system analysis
  Requires --times= for number of times to repeat
  Requires --period= for time period between repetition
placement: !!str run
package:
  - !!str
language: !!str bash
content: !!str |
  #!/bin/bash
  error_trap()
  {
      printf "%0.s=" {1..80}
      echo -e "\nERROR: "$BASH_COMMAND" exited with an error on line ${BASH_LINENO[0]}"
      exit 0
  }
  trap error_trap ERR

  # read-in shared function
  source functions.bash
  echo "I will collect ps output from this $EC2RL_DISTRO box for $times times every
 $period seconds."
  for i in $(seq 1 $times); do
      ps auxww
      sleep $period
  done
constraint:
  requires_ec2: !!str False
  domain: !!str performance
  class: !!str collect
  distro: !!str alami ubuntu rhel suse
  required: !!str period times
  optional: !!str
  software: !!str
  sudo: !!str False
  perfimpact: !!str False
  parallelexclusive: !!str
```

Utilizar EC2Rescue for Windows Server

EC2Rescue for Windows Server es una herramienta fácil de utilizar que se ejecuta en una instancia de Windows Server de Amazon EC2 para diagnosticar y solucionar posibles problemas. Es muy útil para recopilar archivos de registro y solucionar problemas, además de buscar proactivamente posibles áreas problemáticas. Incluso puede examinar volúmenes raíz de Amazon EBS de otras instancias y recopilar los registros pertinentes para solucionar problemas en las instancias de Windows Server que utilizan dichos volúmenes.

EC2Rescue for Windows Server consta de dos módulos: un módulo de recopilación de datos que recopila datos de todas las fuentes y un módulo de análisis que analiza los datos recogidos comparándolos con una serie de reglas predefinidas para detectar problemas y ofrecer sugerencias.

La herramienta EC2Rescue para Windows Server solo se ejecuta en instancias de Amazon EC2 con Windows Server 2012 y versiones posteriores. Cuando se inicia la herramienta, comprueba si está ejecutándose en una instancia de Amazon EC2.

El runbook `AWSSupport-ExecuteEC2Rescue` utiliza la herramienta EC2Rescue para solucionar problemas y, en la medida de lo posible, reparar problemas de conectividad comunes con la instancia EC2 especificada. Para obtener más información y ejecutar esta automatización, consulte AWSSupport-ExecuteEC2rescate.

Si usa una instancia de Linux, consulte the section called “EC2Rescue for Linux”.

Contenido

Utilizar EC2Rescue for Windows Server GUI

EC2Rescue for Windows Server puede realizar el análisis siguiente en instancias sin conexión:

Opción	Descripción
Diagnose and Rescue (Diagnóstico y rescate)	EC2Rescue for Windows Server puede detectar y resolver problemas con la siguiente configuración de servicio:

Opción	Descripción

	• Hora del sistema
	  • RealTimeisUniversal: detecta si la clave de registro `RealTimeisUniversal` está habilitada. Si está deshabilitada, la hora del sistema Windows varía cuando la zona horaria se establece en un valor que no es UTC.
	• Firewall de Windows
	  • Domain networks (Redes de dominio): detecta si este perfil de firewall de Windows está habilitado o no.
	  • Private networks (Redes privadas): detecta si este perfil de firewall de Windows está habilitado o no.
	  • Guest or public networks (Redes públicas o de invitados): detecta si este perfil de firewall de Windows está habilitado o no.
	• Escritorio remoto
	  • Service Start (Inicio de servicio): detecta si el servicio de escritorio remoto está habilitado.
	  • Remote Desktop Connections (Conexiones de escritorio remoto): detecta si esta opción está habilitada.
	  • TCP Port (Puerto TCP): detecta el puerto en el que escucha el servicio de escritorio remoto.
	• EC2Config (Windows Server 2012 R2 y versiones anteriores)

Opción	Descripción
	• Installation (Instalación): detecta la versión de EC2Config que está instalada. • Service Start (Inicio de servicio): detecta si el servicio de EC2Config está habilitado. • Ec2SetPassword: genera una contraseña de administrador nueva. • Ec2HandleUserData: permite ejecutar un script de datos de usuario en el siguiente arranque de la instancia. • EC2Launch (Windows Server 2016 y versiones posteriores) • Installation (Instalación): detecta la versión de EC2Launch que está instalada. • Ec2SetPassword: genera una contraseña de administrador nueva. • Interfaz de red • DHCP Service Startup (Inicio del servicio DHCP): detecta si el servicio DHCP está habilitado. • Ethernet detail (Detalles de Ethernet): muestra información sobre la versión del controlador de red, si se detecta. • DHCP on Ethernet (DHCP en Ethernet): detecta si el servicio DHCP está habilitado. • Estado de firma de disco • Firma en disco y Firma en la base de datos de configuración de arranque (BCD): detecta si la firma del disco y la firma BCD son las mismas. Si los valores son

Opción	Descripción
	diferentes, EC2Rescue intenta sobrescribir la firma del disco con la firma en BCD.
Restaurar	Lleve a cabo una de las siguientes acciones: • Last Known Good Configuration (Última configuración correcta conocida): intenta arrancar la instancia en el último estado de arranque conocido. • Restore registry from backup (Restaurar registro a partir de una copia de seguridad): restaura el registro a partir de `\Windows\System32\config\RegBack` .
Capture Logs (Captura de registros)	Permite capturar registros en la instancia para analizarlos.

EC2Rescue for Windows Server puede recopilar los datos siguientes en las instancias activas y sin conexión:

Elemento	Descripción
Event Log (Registro de eventos)	Recopila los registros de eventos de aplicación, sistema y EC2Config.
Registry (Registro)	Recopila los hives `SYSTEM` y `SOFTWARE`.
Windows Update Log (Registro de Windows Update)	Recopila los archivos de registro generados por Windows Update. **Note** En Windows Server 2016 y versiones posteriores, el registro se recopila en formato de seguimiento de eventos

Elemento	Descripción
	para Windows (ETW, Event Tracing for Windows).
Sysprep Log (Registro de Sysprep)	Recopila los archivos de registro generados por la herramienta Windows System Preparation.
Registro de configuración del controlador	Recopila los registros de Windows SetupAPI (`setupapi.dev.log` y `setupapi.setup.log`).
Boot Configuration (Configuración de arranque)	Recopila el hive `HKEY_LOCAL_MACHINE\BCD00000000`.
Memory Dump (Volcado de memoria)	Recopila los archivos de volcado de memoria que existen en la instancia.
EC2Config File (Archivo de EC2Config)	Recopila los archivos de registro generados por el servicio EC2Config.
EC2Launch File (Archivo de EC2Launch)	Recopila los archivos de registro generados por los scripts de EC2Launch.
SSM Agent File (Archivo del agente de SSM)	Recopila los archivos de registro generados por los registros del SSM Agent y del administrador de parches.
Archivo ElasticGPU EC2	Recopila los registros de eventos relacionados con las GPU elásticas.
ECS	Recopila registros relacionados con Amazon ECS.
CloudEndure	Recopila archivos de registro relacionados con el agente de CloudEndure.

EC2Rescue for Windows Server puede recopilar los siguientes datos adicionales de instancias activas:

Elemento	Descripción
System Information (Información del sistema)	Recopila MSInfo32.
Resultado de política de grupo	Recopila el informe de una política de grupo.

Analizar una instancia sin conexión

La opción Offline Instance (Instancia sin conexión) es útil para depurar problemas de arranque con instancias de Windows.

Para ejecutar una acción en una instancia sin conexión

1. Desde una instancia de Windows Server activa, descargue la herramienta EC2Rescue for Windows Server y extraiga los archivos.

   Puede ejecutar el siguiente comando de PowerShell para descargar EC2Rescue sin cambiar la Configuración de seguridad mejorada (ESC) de Internet Explorer.

   ```
   Invoke-WebRequest https://s3.amazonaws.com/ec2rescue/windows/EC2Rescue_latest.zip -
   OutFile $env:USERPROFILE\Desktop\EC2Rescue_latest.zip
   ```

   Este comando descargará el archivo .zip de EC2Rescue en el escritorio del usuario que haya iniciado sesión actualmente

   > **Note**
   >
   > Si recibe un error al descargar el archivo y está usando Windows Server 2016 o una versión anterior, es posible que sea necesario habilitar TLS 1.2 para su terminal PowerShell. Puede habilitar TLS 1.2 para la sesión actual de PowerShell con el siguiente comando y luego volver a intentarlo:

```
[Net.ServicePointManager]::SecurityProtocol =
 [Net.SecurityProtocolType]::Tls12
```

2. Detenga la instancia que tiene el problema si todavía no la ha detenido.
3. Separe el volumen raíz de EBS de la instancia con problemas y adjunte el volumen a la instancia de Windows activa que tenga EC2Rescue for Windows Server instalado.
4. Ejecute la herramienta EC2Rescue for Windows Server en la instancia activa y elija Offline Instance (Instancia sin conexión).
5. Seleccione el disco del volumen que acaba de montar y elija Next (Siguiente).
6. Confirme la selección del disco y elija Yes (Sí).
7. Elija la opción de instancia sin conexión que debe ejecutarse y elija Next (Siguiente).

La herramienta EC2Rescue for Windows Server analiza el volumen y recopila información de solución de problemas basándose en los archivos de registro seleccionados.

Para recopilar datos de una instancia activa

Puede recopilar registros y demás datos de una instancia activa.

Para recopilar datos de una instancia activa

1. Conéctese a la instancia de Windows.
2. Descargue la herramienta EC2Rescue for Windows Server en su instancia de Windows y extraiga los archivos.

   Puede ejecutar el siguiente comando de PowerShell para descargar EC2Rescue sin cambiar la Configuración de seguridad mejorada (ESC) de Internet Explorer.

   ```
   Invoke-WebRequest https://s3.amazonaws.com/ec2rescue/windows/EC2Rescue_latest.zip -
   OutFile $env:USERPROFILE\Desktop\EC2Rescue_latest.zip
   ```

   Este comando descargará el archivo .zip de EC2Rescue en el escritorio del usuario que haya iniciado sesión actualmente

> **Note**
>
> Si recibe un error al descargar el archivo y está usando Windows Server 2016 o una versión anterior, es posible que sea necesario habilitar TLS 1.2 para su terminal PowerShell. Puede habilitar TLS 1.2 para la sesión actual de PowerShell con el siguiente comando y luego volver a intentarlo:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol =
>  [Net.SecurityProtocolType]::Tls12
> ```

3. Abra la aplicación EC2Rescue for Windows Server y acepte el acuerdo de licencia.
4. Elija Next (Siguiente), Current instance (Instancia actual), Capture logs (Capturar registros).
5. Seleccione los elementos de datos que deben recopilarse y elija Collect (Recopilar). Lea la advertencia y seleccione Yes (Sí) para continuar.
6. Elija un nombre de archivo y una ubicación para el archivo ZIP y elija Save (Guardar).
7. Una vez que EC2Rescue for Windows Server se haya completado, elija Open Containing Folder (Abrir carpeta contenedora) para ver el archivo ZIP.
8. Elija Finalizar.

Utilizar EC2Rescue for Windows Server con la línea de comando

La interfaz de línea de comandos (CLI) de EC2Rescue for Windows Server permite ejecutar el complemento EC2Rescue for Windows Server (denominado "acción") mediante programación.

La herramienta EC2Rescue for Windows Server cuenta con dos modos de ejecución:

- /online: permite realizar acciones en la instancia donde está instalado EC2Rescue for Windows Server, como recopilar archivos de registro.
- /offline<device_id>: permite realizar acciones en el volumen raíz sin conexión adjunto a una instancia de Windows de Amazon EC2 independiente en la que se haya instalado EC2Rescue for Windows Server.

Descargue la herramienta EC2Rescue for Windows Server en su instancia de Windows y extraiga los archivos. Puede ver el archivo de ayuda con el comando siguiente:

```
EC2RescueCmd.exe /help
```

EC2Rescue for Windows Server puede realizar las acciones siguientes en una instancia de Windows de Amazon EC2:

- Acción de recopilación
- Acción de rescate
- Acción de restauración

Acción de recopilación

> **Note**
>
> Se pueden recopilar todos los registros, un grupo entero de registros o un solo registro de un grupo.

EC2Rescue for Windows Server puede recopilar los datos siguientes en las instancias activas y sin conexión.

Grupo de registros	Registros disponibles	Descripción
`all`		Recopila todos los registros disponibles.
`eventlog`	• `'Application'` • `'System'` • `'EC2ConfigService'`	Recopila los registros de eventos de aplicación, sistema y EC2Config.
`memory-dump`	• `'Memory Dump File'` • `'Mini Dump Files'`	Recopila los archivos de volcado de memoria que existen en la instancia.
`ec2config`	• `'Log Files'` • `'Configuration Files'`	Recopila los archivos de registro generados por el servicio EC2Config.

Grupo de registros	Registros disponibles	Descripción
ec2launch	• 'Logs' • 'Config'	Recopila los archivos de registro generados por los scripts de EC2Launch.
ssm-agent	• 'Log Files' • 'Patch Baseline Logs' • 'InstanceData'	Recopila los archivos de registro generados por los registros del SSM Agent y del administrador de parches.
sysprep	'Log Files'	Recopila los archivos de registro generados por la herramienta Windows System Preparation.
driver-setup	• 'SetupAPI Log Files' • 'DPInst Log File' • 'AWS PV Setup Log File'	Recopila los registros de Windows SetupAPI (setupapi.dev.log y setupapi.setup.log).
registry	• 'SYSTEM' • 'SOFTWARE' • 'BCD'	Recopila los hives SYSTEM y SOFTWARE.
egpu	• 'Event Log' • 'System Files'	Recopila los registros de eventos relacionados con las GPU elásticas.
boot-config	'BCDEDIT Output'	Recopila el hive HKEY_LOCAL_MACHINE\BCD00000000 .

Grupo de registros	Registros disponibles	Descripción
`windows-update`	`'Log Files'`	Recopila los archivos de registro generados por Windows Update. **Note** En Windows Server 2016 y versiones posteriores, el registro se recopila en formato de seguimiento de eventos para Windows (ETW, Event Tracing for Windows).
`cloudendure`	• `'Migrate Script Logs'` • `'Driver Logs'` • `'CloudEndure File List'`	Recopila archivos de registro relacionados con el agente de CloudEndure.

EC2Rescue for Windows Server puede recopilar los siguientes datos adicionales de instancias activas.

Grupo de registros	Registros disponibles	Descripción
`system-info`	`'MSInfo32 Output'`	Recopila `MSInfo32`.
`gpresult`	`'GPResult Output'`	Recopila el informe de una política de grupo.

Están disponibles las siguientes opciones:

- /output:<outputFilePath>: ubicación de ruta obligatoria del archivo de destino donde se guardan los archivos de registro recopilados en formato zip.
- /no-offline: atributo opcional que se utiliza en el modo sin conexión. No configura el volumen como sin conexión después de realizar la acción.
- /no-fix-signature: atributo opcional que se utiliza en el modo sin conexión. No corrige el posible conflicto de firmas de disco después de realizar la acción.

Ejemplos

A continuación se muestran ejemplos del uso de la CLI de EC2Rescue for Windows Server.

Ejemplos del modo online

Recopila todos los registros disponibles:

```
EC2RescueCmd /accepteula /online /collect:all /output:<outputFilePath>
```

Solo recopila un grupo de registros concreto:

```
EC2RescueCmd /accepteula /online /collect:ec2config /output:<outputFilePath>
```

Recopila registros concretos de un grupo de registros:

```
EC2RescueCmd /accepteula /online /collect:'ec2config.Log Files,driver-setup.SetupAPI
 Log Files' /output:<outputFilePath>
```

Ejemplos del modo sin conexión

Recopila todos los registros disponibles de un volumen de EBS. El volumen se especifica con el valor de id_dispositivo.

```
EC2RescueCmd /accepteula /offline:xvdf /collect:all /output:<outputFilePath>
```

Solo recopila un grupo de registros concreto:

```
EC2RescueCmd /accepteula /offline:xvdf /collect:ec2config /output:<outputFilePath>
```

Acción de rescate

EC2Rescue for Windows Server puede detectar y resolver problemas con la siguiente configuración de servicio:

Grupo de servicios	Acciones disponibles	Descripción
`all`		
`system-time`	`'RealTimeIsUniversal'`	Hora del sistema • RealTimeisUniversal: detecta si la clave de registro `RealTimeisUniversal` está habilitada. Si está deshabilitada, la hora del sistema Windows varía cuando la zona horaria se establece en un valor que no es UTC.
`firewall`	• `'Domain networks'` • `'Private networks'` • `'Guest or public networks'`	Firewall de Windows • Domain networks (Redes de dominio): detecta si este perfil de firewall de Windows está habilitado o no. • Private networks (Redes privadas): detecta si este perfil de firewall de Windows está habilitado o no. • Guest or public networks (Redes públicas o de invitados): detecta si este perfil de firewall de Windows está habilitado o no.
rdp	• `'Service Start'`	Escritorio remoto

Grupo de servicios	Acciones disponibles	Descripción
	• 'Remote Desktop Connections' • 'TCP Port'	• Service Start (Inicio de servicio): detecta si el servicio de escritorio remoto está habilitado. • Remote Desktop Connections (Conexiones de escritorio remoto): detecta si esta opción está habilitada. • TCP Port (Puerto TCP): detecta el puerto en el que escucha el servicio de escritorio remoto.
ec2config	• 'Service Start' • 'Ec2SetPassword' • 'Ec2HandleUserData'	EC2Config • Service Start (Inicio de servicio): detecta si el servicio de EC2Config está habilitado. • Ec2SetPassword: genera una contraseña de administrador nueva. • Ec2HandleUserData: permite ejecutar un script de datos de usuario en el siguiente arranque de la instancia.
ec2launch	'Reset Administrator Password'	Genera una contraseña de administrador de Windows nueva.

Grupo de servicios	Acciones disponibles	Descripción
`network`	`'DHCP Service Startup'`	Interfaz de red • DHCP Service Startup (Inicio del servicio DHCP): detecta si el servicio DHCP está habilitado.

Están disponibles las siguientes opciones:

- /level:<level>: atributo opcional correspondiente al nivel de verificación que debe disparar la acción. Los valores permitidos son: `information`, `warning`, `error`, `all`. De forma predeterminada, está establecido en `error`.
- /check-only: atributo opcional que genera un informe, pero no realiza ninguna modificación en el volumen sin conexión.

> **Note**
>
> Si EC2Rescue for Windows Server detecta una posible colisión de firmas en el disco, corrige la firma una vez finalizado el proceso sin conexión de forma predeterminada, incluso si utiliza la opción `/check-only`. Debe utilizar la opción `/no-fix-signature` para impedir la corrección.

- /no-offline: atributo opcional que impide que el volumen se configure como sin conexión después de realizar la acción.
- /no-fix-signature: atributo opcional que no corrige el posible conflicto de firmas de disco después de realizar la acción.

Ejemplos de rescate

A continuación se muestran ejemplos del uso de la CLI de EC2Rescue for Windows Server. El volumen se especifica con el valor de id_dispositivo.

Intenta corregir todos los problemas identificados en un volumen:

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:all
```

Intenta corregir todos los problemas de un grupo de servicios de un volumen:

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:firewall
```

Intenta corregir un elemento concreto de un grupo de servicios de un volumen:

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:rdp.'Service Start'
```

Especifica los distintos problemas que se deben intentar corregir en un volumen:

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:'system-
time.RealTimeIsUniversal,ec2config.Service Start'
```

Acción de restauración

EC2Rescue for Windows Server puede detectar y resolver problemas con la siguiente configuración de servicio:

Grupo de servicios	Acciones disponibles	Descripción
Restaurar la última configuración correcta conocida	`lkgc`	Last Known Good Configuration (Última configuración correcta conocida): intenta arrancar la instancia en el último estado de arranque conocido.
Restaurar el Registro de Windows a partir del último backup	`regback`	Restore registry from backup (Restaurar registro a partir de una copia de seguridad): restaura el registro a partir de `\Windows\System32\config\RegBack` .

Están disponibles las siguientes opciones:

- /no-offline: atributo opcional para impedir que el volumen se configure como sin conexión después de realizar la acción.

- /no-fix-signature: atributo opcional que no corrige el posible conflicto de firmas de disco después de realizar la acción.

Ejemplos de restauración

A continuación se muestran ejemplos del uso de la CLI de EC2Rescue for Windows Server. El volumen se especifica con el valor de id_dispositivo.

Restaura la última configuración correcta conocida en un volumen:

```
EC2RescueCmd /accepteula /offline:xvdf /restore:lkgc
```

Restaura el último backup del Registro de Windows en un volumen:

```
EC2RescueCmd /accepteula /offline:xvdf /restore:regback
```

Utilizar EC2Rescue for Windows Server con Run Command de Systems Manager

AWS Support proporciona un documento de Systems Manager Run Command que facilita la ejecución de Systems Manager en la instancia habilitada para EC2Rescue for Windows Server. El documento de Run Command se llama `AWSSupport-RunEC2RescueForWindowsTool`.

Este documento Run Command de Systems Manager realiza las tareas siguientes:

- Descarga y verifica EC2Rescue for Windows Server.
- Importa un módulo de PowerShell que facilita la interacción con la herramienta.
- Ejecuta EC2RescueCmd con los comandos y los parámetros proporcionados.

El documento Run Command de Systems Manager acepta tres parámetros:

- Command (Comando): acción de EC2Rescue for Windows Server. Estos son los valores que se permiten actualmente:
  - ResetAccess: restablece la contraseña del administrador local. Se restablece la contraseña del administrador local de la instancia actual y la contraseña aleatoria generada se almacena de forma segura como en Parameter Stor `/EC2Rescue/Password/<INSTANCE_ID>`.

Si selecciona esta acción, pero no proporciona ningún parámetro, la contraseña se cifra automáticamente con la Clave de KMS predeterminada. También tiene la opción de especificar un ID de Clave de KMS en Parameters (Parámetros) para cifrar la contraseña con su propia clave.

- CollectLogs: ejecuta EC2Rescue for Windows Server con la acción `/collect:all`. Si selecciona esta acción, `Parameters` debe incluir un nombre de bucket de Amazon S3 para cargar los registros.
- FixAll: ejecuta EC2Rescue for Windows Server con la acción `/rescue:all`. Si selecciona esta acción, `Parameters` debe incluir el nombre del dispositivo de bloques que se tiene que rescatar.

- Parameters (Parámetros): parámetros de PowerShell que se deben pasar al comando especificado.

Note

Para que la acción ResetAccess funcione, la instancia de Amazon EC2 debe tener asociada la política siguiente, que permite escribir la contraseña cifrada en Parameter Store. Después de adjuntar esta política al rol de IAM relacionado, espere unos minutos antes de intentar restablecer la contraseña de la instancia.
Uso de la Clave de KMS predeterminada:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:PutParameter"
      ],
      "Resource": [
        "arn:aws:ssm:region:account_id:parameter/EC2Rescue/
Passwords/<instanceid>"
      ]
    }
  ]
}
```

Uso de una Clave de KMS personalizada:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:PutParameter"
      ],
      "Resource": [
        "arn:aws:ssm:region:account_id:parameter/EC2Rescue/
Passwords/<instanceid>"
        ]
      },
      {
      "Effect": "Allow",
      "Action": [
      "kms:Encrypt"
      ],
      "Resource": [
        "arn:aws:kms:region:account_id:key/<kmskeyid>"
      ]
    }
  ]
}
```

En el siguiente procedimiento se describe cómo ver el código JSON de este documento en la consola de Amazon EC2.

Para ver el código JSON del documento Run Command de Systems Manager

1. Abra la consola de Systems Manager en https://console.aws.amazon.com/systems-manager/home.
2. En el panel de navegación, expanda Shared Services (Servicios compartidos) y elija Documents (Documentos).
3. En la barra de búsqueda, establezca Owner (Propietario) en Owned by Me or Amazon (De mi propiedad o de Amazon) y Document name prefix (Prefijo de nombre de documento) en `AWSSupport-RunEC2RescueForWindowsTool`.

4. Seleccione el documento `AWSSupport-RunEC2RescueForWindowsTool`, elija Contents (Contenido) y, a continuación, consulte el código JSON.

Ejemplos

A continuación, se ofrecen algunos ejemplos sobre cómo utilizar el documento de Systems Manager Run Command para ejecutar EC2Rescue for Windows Server, mediante AWS CLI. Para obtener más información sobre el envío de comandos con la AWS CLI, consulte AWS CLI Command Reference.

Intenta corregir todos los problemas identificados en un volumen raíz sin conexión

Intenta corregir todos los problemas identificados en un volumen raíz sin conexión adjunto a una instancia de Windows de Amazon EC2:

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-
RunEC2RescueForWindowsTool" --comment "EC2Rescue offline volume xvdf" --parameters
 "Command=FixAll, Parameters='xvdf'" --output text
```

Recopilación de registros de la instancia de Windows de Amazon EC2 actual

Recopila todos los registros de la instancia actual online de Windows de Amazon EC2 y los carga en un bucket de Amazon S3:

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-
RunEC2RescueForWindowsTool" --comment "EC2Rescue online log collection to S3" --
parameters "Command=CollectLogs, Parameters='YOURS3BUCKETNAME'" --output text
```

Recopilación de registros de una instancia de Windows de Amazon EC2 sin conexión

Recopila todos los registros de un volumen sin conexión adjunto a una instancia de Windows de Amazon EC2 y los carga en Amazon S3 con una URL prefirmada:

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-
RunEC2RescueForWindowsTool" --comment "EC2Rescue offline log collection to S3"
 --parameters "Command=CollectLogs, Parameters=\"-Offline -BlockDeviceName xvdf -
S3PreSignedUrl 'YOURS3PRESIGNEDURL'\"" --output text
```

Restablecimiento de la contraseña del administrador local

En los ejemplos siguientes se muestran los métodos que sirven para restablecer la contraseña del administrador local. La salida incluye un enlace a Parameter Store, donde se encuentra la

contraseña aleatoria segura generada que permite conectar con RDP como administrador local a la instancia de Windows de Amazon EC2.

Restablecimiento de la contraseña del administrador local de una instancia online con la AWS KMS key predeterminada, alias/aws/ssm:

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-
RunEC2RescueForWindowsTool" --comment "EC2Rescue online password reset" --parameters
 "Command=ResetAccess" --output text
```

Restablecimiento de la contraseña del administrador local de una instancia online con una Clave de KMS:

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-
RunEC2RescueForWindowsTool" --comment "EC2Rescue online password reset" --parameters
 "Command=ResetAccess, Parameters=a133dc3c-a2g4-4fc6-a873-6c0720104bf0" --output text
```

> **Note**
>
> En este ejemplo, la Clave de KMS es `a133dc3c-a2g4-4fc6-a873-6c0720104bf0`.

Consola serie de EC2 para instancias de Amazon EC2

Con la consola serie de EC2, tiene acceso al puerto serie de la instancia de Amazon EC2, que puede utilizar para solucionar problemas de arranque, configuración de red y otros problemas. La consola serie no requiere que la instancia tenga ninguna capacidad de red. Con la consola serie, puede introducir comandos en una instancia como si el teclado y el monitor estuvieran conectados directamente al puerto serie de la instancia. La sesión de la consola serie dura durante el reinicio y la detención de la instancia. Durante el reinicio, puede ver todos los mensajes de arranque desde el inicio.

El acceso a la consola serie no está disponible de forma predeterminada. La organización debe conceder acceso a la cuenta a la consola serie y configurar políticas de IAM para otorgar a los usuarios acceso a la consola serie. El acceso a la consola serie se puede controlar a nivel granular mediante ID de instancia, etiquetas de recursos y otras palancas de IAM. Para obtener más información, consulte Configurar el acceso a la consola serie de EC2.

Se puede acceder a la consola serie mediante la consola de EC2 o la AWS CLI.

La consola serie está disponible sin costo adicional.

Temas

Requisitos previos

Para conectarse a la consola serie de EC2 y utilizar la herramienta elegida para la solución de problemas, deben existir los requisitos previos siguientes:

- Regiones de AWS
- Zonas Wavelength y AWS Outposts
- Zonas locales
- Tipos de instancias
- Conceder acceso
- Soporte para cliente basado en navegador
- Estado de la instancia
- Amazon EC2, Systems Manager
- servidor sshd
- Configuración de la herramienta de solución de problemas elegida

Regiones de AWS

Se admite en todas las Regiones de AWS, excepto en Oeste de Canadá (Calgary).

Zonas Wavelength y AWS Outposts

No admitido.

Zonas locales

No se admite en zonas locales.

Tipos de instancias

Tipos de instancias admitidas:

- Linux
  - Todas las instancias virtualizadas integradas en el sistema Nitro.
  - Todas las instancias bare metal, excepto:
    - De uso general: `a1.metal`, `mac1.metal`, `mac2.metal`
    - Computación acelerada: `g5g.metal`
    - Memoria optimizada: `u-6tb1.metal`, `u-9tb1.metal`, `u-12tb1.metal`, `u-18tb1.metal`, `u-24tb1.metal`
- Windows

  Todas las instancias virtualizadas integradas en el sistema Nitro. No es compatible con instancias bare metal.

Conceder acceso

Debe completar las tareas de configuración para otorgar acceso a la consola serie de EC2. Para obtener más información, consulte Configurar el acceso a la consola serie de EC2.

Soporte para cliente basado en navegador

Para conectarse a la consola serie con el cliente basado en navegador, su navegador debe admitir WebSocket. Si su navegador no admite WebSocket, conéctese a la consola serie con su propia clave y un cliente SSH.

Estado de la instancia

Debe ser `running`.

Si la instancia está en estado `pending`, `stopping`, `stopped`, `shutting-down` o `terminated`, no puede conectarse a la consola serie.

Para obtener más información acerca de los estados de las instancias, consulte Ciclo de vida de la instancia.

Amazon EC2, Systems Manager

Si la instancia utiliza Amazon EC2 Systems Manager, debe instalarse en la instancia la versión 3.0.854.0 de SSM Agent o una posterior. Para obtener más información acerca de SSM Agent, consulte Uso de SSM Agent en la Guía del usuario de AWS Systems Manager.

servidor sshd

No necesita un servidor sshd instalado o ejecutándose en su instancia.

Configuración de la herramienta de solución de problemas elegida

instancias de Linux

Para solucionar problemas de la instancia de Linux a través de la consola serie, puede usar GRUB o SysRQ. Antes de poder utilizar estas herramientas, primero debe realizar los pasos de configuración en cada instancia en la que las vaya a utilizar.

Herramientas

- Configurar GRUB
- Configurar SysRq

Configurar GRUB

Antes de poder utilizar GRUB a través de la consola serie, debe configurar su instancia para que use GRUB a través de la consola serie.

Para configurar GRUB, elija uno de los siguientes procedimientos basados en la AMI que se utilizó para iniciar la instancia.

Amazon Linux 2

Para configurar GRUB en una instancia de Amazon Linux 2

1. Conexión con la instancia de Linux
2. Agregue o cambie las siguientes opciones en `/etc/default/grub`:
   - Configurar `GRUB_TIMEOUT=1`.
   - Add `GRUB_TERMINAL="console serial"`.

- Añada `GRUB_SERIAL_COMMAND="serial --speed=115200"`.

A continuación se muestra un ejemplo de `/etc/default/grub`. Es posible que tenga que cambiar la configuración en función de la configuración del sistema.

```
GRUB_CMDLINE_LINUX_DEFAULT="console=tty0 console=ttyS0,115200n8 net.ifnames=0
 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff rd.shell=0"
GRUB_TIMEOUT=1
GRUB_DISABLE_RECOVERY="true"
GRUB_TERMINAL="console serial"
GRUB_SERIAL_COMMAND="serial --speed=115200"
```

3. Aplique la configuración actualizada ejecutando el siguiente comando.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

Ubuntu

Para configurar GRUB en una instancia de Ubuntu

1. Conéctese a la instancia.
2. Agregue o cambie las siguientes opciones en `/etc/default/grub.d/50-cloudimg-settings.cfg`:
   - Configurar `GRUB_TIMEOUT=1`.
   - Add `GRUB_TIMEOUT_STYLE=menu`.
   - Añada `GRUB_TERMINAL="console serial"`.
   - Remove `GRUB_HIDDEN_TIMEOUT`.
   - Añada `GRUB_SERIAL_COMMAND="serial --speed=115200"`.

   A continuación se muestra un ejemplo de `/etc/default/grub.d/50-cloudimg-settings.cfg`. Es posible que tenga que cambiar la configuración en función de la configuración del sistema.

```
# Cloud Image specific Grub settings for Generic Cloud Images
# CLOUD_IMG: This file was created/modified by the Cloud Image build process
```

```
# Set the recordfail timeout
GRUB_RECORDFAIL_TIMEOUT=0

# Do not wait on grub prompt
GRUB_TIMEOUT=1
GRUB_TIMEOUT_STYLE=menu

# Set the default commandline
GRUB_CMDLINE_LINUX_DEFAULT="console=tty1 console=ttyS0
 nvme_core.io_timeout=4294967295"

# Set the grub console type
GRUB_TERMINAL="console serial"
GRUB_SERIAL_COMMAND="serial --speed 115200"
```

3. Aplique la configuración actualizada ejecutando el siguiente comando.

```
[ec2-user ~]$ sudo update-grub
```

RHEL

Para configurar GRUB en una instancia de RHEL

1. Conéctese a la instancia.
2. Agregue o cambie las siguientes opciones en `/etc/default/grub`:
   - Remove `GRUB_TERMINAL_OUTPUT`.
   - Add `GRUB_TERMINAL="console serial"`.
   - Añada `GRUB_SERIAL_COMMAND="serial --speed=115200"`.

   A continuación se muestra un ejemplo de `/etc/default/grub`. Es posible que tenga que cambiar la configuración en función de la configuración del sistema.

```
GRUB_TIMEOUT=1
GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
GRUB_DEFAULT=saved
GRUB_DISABLE_SUBMENU=true
GRUB_CMDLINE_LINUX="console=tty0 console=ttyS0,115200n8 net.ifnames=0
 rd.blacklist=nouveau nvme_core.io_timeout=4294967295 crashkernel=auto"
GRUB_DISABLE_RECOVERY="true"
```

```
GRUB_ENABLE_BLSCFG=true
GRUB_TERMINAL="console serial"
GRUB_SERIAL_COMMAND="serial --speed=115200"
```

3. Aplique la configuración actualizada ejecutando el siguiente comando.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

CentOS

Para las instancias que se inician mediante una AMI de CentOS, GRUB está configurado para la consola serie de forma predeterminada.

A continuación se muestra un ejemplo de `/etc/default/grub`. La configuración puede ser diferente en función de la configuración del sistema.

```
GRUB_TIMEOUT=1
GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
GRUB_DEFAULT=saved
GRUB_DISABLE_SUBMENU=true
GRUB_TERMINAL="serial console"
GRUB_SERIAL_COMMAND="serial --speed=115200"
GRUB_CMDLINE_LINUX="console=tty0 crashkernel=auto console=ttyS0,115200"
GRUB_DISABLE_RECOVERY="true"
```

Configurar SysRq

Para configurar SysRq, habilite los comandos SysRq para el ciclo de arranque actual. Para que la configuración sea persistente, también puede habilitar los comandos SysRq para los siguientes arranques.

Para habilitar todos los comandos SysRq para el ciclo de arranque actual

1. Conéctese a la instancia.
2. Ejecute el siguiente comando.

```
[ec2-user ~]$ sudo sysctl -w kernel.sysrq=1
```

> **Note**
>
> Esta configuración se borrará en el próximo reinicio.

Para habilitar todos los comandos SysRq para los siguientes arranques

1. Cree el archivo `/etc/sysctl.d/99-sysrq.conf` y ábralo en su editor favorito.

```
[ec2-user ~]$ sudo vi /etc/sysctl.d/99-sysrq.conf
```

2. Añada la siguiente línea.

```
kernel.sysrq=1
```

3. Reinicie la instancia para aplicar los cambios.

```
[ec2-user ~]$ sudo reboot
```

4. En la solicitud `login`, escriba el nombre de usuario del usuario basado en contraseña que configuró anteriormente y, a continuación, presione Enter (Entrar).
5. En la solicitud `Password`, escriba la contraseña y, a continuación, presione Enter (Entrar).

instancias de Windows

Para solucionar problemas de la instancia de Windows mediante la consola serie, puede usar la consola de administración especial (SAC). Antes de poder utilizar la SAC, primero debe habilitar la SAC y el menú de arranque en cada instancia en la que vaya a usarla.

Habilitar SAC y el menú de inicio

> **Note**
>
> Si habilita SAC en una instancia, los servicios de EC2 que dependen de la recuperación de contraseñas no funcionarán desde la consola de Amazon EC2. Los agentes de lanzamiento de Windows en Amazon EC2 (EC2Config, EC2Launch v1 y EC2Launch v2) dependen de la consola serie para ejecutar diversas tareas. Esas tareas no se ejecutan correctamente cuando se habilita SAC en una instancia. Para obtener más información sobre los agentes

de lanzamiento de Windows en Amazon EC2, consulte the section called “Configuración de instancias de Windows”. Si habilita SAC, podrá desactivarlo más adelante. Para obtener más información, consulte Desactivar SAC y el menú de inicio.

Utilice uno de los métodos siguientes para habilitar SAC y el menú de arranque en una instancia.

PowerShell

Para habilitar SAC y el menú de inicio en una instancia de Windows

1. Conéctese a la instancia y realice los siguientes pasos desde la línea de comandos elevada de PowerShell.
2. Habilite SAC.

```
bcdedit /ems '{current}' on
bcdedit /emssettings EMSPORT:1 EMSBAUDRATE:115200
```

3. Habilite el menú de inicio.

```
bcdedit /set '{bootmgr}' displaybootmenu yes
bcdedit /set '{bootmgr}' timeout 15
bcdedit /set '{bootmgr}' bootems yes
```

4. Aplique la configuración actualizada reiniciando la instancia.

```
shutdown -r -t 0
```

Command prompt

Para habilitar SAC y el menú de inicio en una instancia de Windows

1. Conéctese a la instancia y realice los siguientes pasos desde el símbolo del sistema.
2. Habilitar SAC.

```
bcdedit /ems {current} on
bcdedit /emssettings EMSPORT:1 EMSBAUDRATE:115200
```

3. Habilite el menú de inicio.

```
bcdedit /set {bootmgr} displaybootmenu yes
bcdedit /set {bootmgr} timeout 15
bcdedit /set {bootmgr} bootems yes
```

4. Aplique la configuración actualizada reiniciando la instancia.

```
shutdown -r -t 0
```

Configurar el acceso a la consola serie de EC2

Para configurar el acceso a la consola serie, debe conceder acceso a la consola serie a nivel de cuenta y, a continuación, configurar políticas de IAM para conceder acceso a los usuarios. Para instancias de Linux, también debe configurar un usuario basado en contraseña en cada instancia a fin de que los usuarios puedan utilizar la consola serie para solucionar problemas.

Antes de empezar, asegúrese de comprobar los prerrequisitos.

Temas

- Niveles de acceso a la consola serie de EC2
- Administrar el acceso a la cuenta a la consola serie de EC2
- Configurar políticas de IAM para el acceso a la consola serie de EC2
- Cómo establecer una contraseña de usuario de SO en una instancia de Linux

Niveles de acceso a la consola serie de EC2

De forma predeterminada, no hay acceso a la consola serie en el nivel de cuenta. Debe conceder explícitamente el acceso a la consola serie en el nivel de cuenta. Para obtener más información, consulte Administrar el acceso a la cuenta a la consola serie de EC2.

Puede utilizar una política de control de servicios (service control policy, SCP) para permitir el acceso a la consola serie dentro de su organización. A continuación, puede tener un control de acceso granular de los usuarios de IAM mediante una política de IAM para controlar el acceso. Al utilizar una combinación de políticas SCP e IAM, tiene diferentes niveles de control de acceso a la consola serie.

Nivel de organización

Puede utilizar una política de control de servicios (SCP) para permitir el acceso a la consola serie para las cuentas de miembros de su organización. Para obtener más información acerca de SCP, consulte Políticas de control de servicios en la Guía del usuario de AWS Organizations.

Nivel de instancia

Puede configurar las políticas de acceso a la consola serie mediante construcciones IAM PrincipalTag y ResourceTag y especificando instancias por su ID. Para obtener más información, consulte Configurar políticas de IAM para el acceso a la consola serie de EC2.

Nivel de usuario

Puede configurar el acceso a nivel de usuario configurando una política de IAM para permitir o denegar a un usuario especificado el permiso para insertar la clave pública SSH al servicio de consola serie de una instancia determinada. Para obtener más información, consulte Configurar políticas de IAM para el acceso a la consola serie de EC2.

Nivel de SO (solo instancias de Linux)

Puede establecer una contraseña de usuario en el nivel del SO invitado. Esto proporciona acceso a la consola serie para algunos casos de uso. Sin embargo, para supervisar los registros, no necesita un usuario basado en contraseña. Para obtener más información, consulte Cómo establecer una contraseña de usuario de SO en una instancia de Linux.

Administrar el acceso a la cuenta a la consola serie de EC2

De forma predeterminada, no hay acceso a la consola serie en el nivel de cuenta. Debe conceder explícitamente el acceso a la consola serie en el nivel de cuenta.

Temas

- Concesión de permisos a los usuarios para administrar el acceso a la cuenta
- Ver el estado de acceso a la cuenta en la consola serie
- Conceder acceso a la cuenta a la consola serie
- Denegar el acceso de cuenta a la consola serie

Concesión de permisos a los usuarios para administrar el acceso a la cuenta

Para permitir que los usuarios administren el acceso a la cuenta en la consola serie de EC2, debe concederles los permisos de IAM necesarios.

La siguiente política concede permisos para ver el estado de la cuenta y para permitir y evitar el acceso de cuenta a la consola serie de EC2.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:GetSerialConsoleAccessStatus",
                "ec2:EnableSerialConsoleAccess",
                "ec2:DisableSerialConsoleAccess"
            ],
            "Resource": "*"
        }
    ]
}
```

Para obtener más información, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

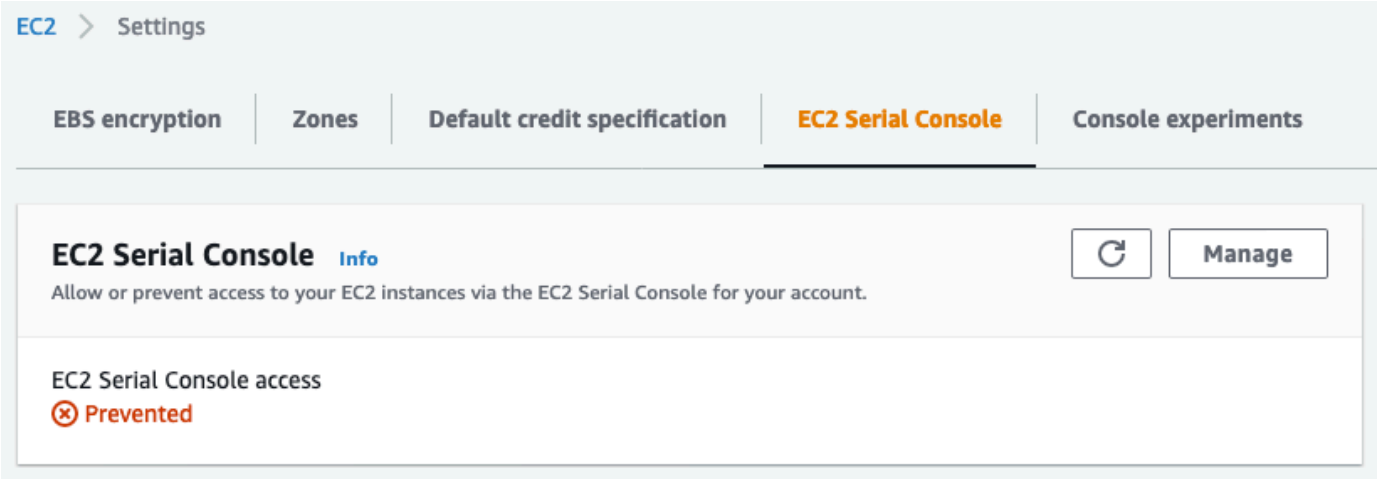
Ver el estado de acceso a la cuenta en la consola serie

Para ver el estado de acceso a la cuenta a la consola serie (consola)

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación izquierdo, elija EC2 Dashboard (Panel de EC2).
3. En Account attributes (Atributos de cuenta), elija EC2 Serial Console (Consola serie de EC2).

   El campo de EC2 Serial Console access (Acceso a la consola serie de EC2) indica si el acceso a la cuenta está Allowed (Permitido) o Prevented (Impedido).

   La siguiente captura de pantalla muestra que la cuenta no puede utilizar la consola serie de EC2.



Para ver el estado de acceso a la cuenta de la consola serie (AWS CLI)

Utilice el comando get-serial-console-access-status para ver el estado de acceso a la cuenta en la consola serie.

```
aws ec2 get-serial-console-access-status --region us-east-1
```

En el siguiente resultado, `true` indica que la cuenta tiene permitido el acceso a la consola serie.

```
{
    "SerialConsoleAccessEnabled": true
}
```

Conceder acceso a la cuenta a la consola serie

Para conceder acceso a la cuenta a la consola serie (consola)

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación izquierdo, elija EC2 Dashboard (Panel de EC2).
3. En Account attributes (Atributos de cuenta), elija EC2 Serial Console (Consola serie de EC2).
4. Seleccione Manage (Administrar).
5. Para permitir el acceso a la consola serie de EC2 de todas las instancias de la cuenta, active la casilla de verificación Allow (Permitir).
6. Elija Update (Actualizar).

Para conceder acceso a la cuenta a la consola serie (AWS CLI)

Utilice el comando enable-serial-console-access para permitir el acceso de cuenta a la consola serie.

```
aws ec2 enable-serial-console-access --region us-east-1
```

En el siguiente resultado, `true` indica que la cuenta tiene permitido el acceso a la consola serie.

```
{
    "SerialConsoleAccessEnabled": true
}
```

Denegar el acceso de cuenta a la consola serie

Para denegar el acceso de cuenta a la consola serie (consola)

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación izquierdo, elija EC2 Dashboard (Panel de EC2).
3. En Account attributes (Atributos de cuenta), elija EC2 Serial Console (Consola serie de EC2).
4. Seleccione Manage (Administrar).
5. Para evitar el acceso a la consola serie de EC2 de todas las instancias de la cuenta, desactive la casilla de verificación Allow (Permitir).
6. Elija Update (Actualizar).

Para denegar el acceso a la cuenta a la consola serie (AWS CLI)

Utilice el comando disable-serial-console-access para impedir el acceso de cuenta a la consola serie.

```
aws ec2 disable-serial-console-access --region us-east-1
```

En el siguiente resultado, `false` indica que se deniega el acceso de la consola serie a la cuenta.

```
{
    "SerialConsoleAccessEnabled": false
}
```

Configurar políticas de IAM para el acceso a la consola serie de EC2

De forma predeterminada, los usuarios no tienen acceso a la consola serie. Su organización debe configurar políticas de IAM para conceder a los usuarios el acceso necesario. Para obtener más información, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Para el acceso a la consola serie, cree un documento de política JSON que incluya la `ec2-instance-connect:SendSerialConsoleSSHPublicKey` acción. Esta acción concede permiso a un usuario para insertar la clave pública en el servicio de consola serie, que inicia una sesión de consola serie. Recomendamos restringir el acceso a instancias de EC2 específicas. De lo contrario, todos los usuarios con este permiso pueden conectarse a la consola serie de todas las instancias de EC2.

Ejemplos de políticas de IAM

- Permitir explícitamente el acceso a la consola serie
- Denegar explícitamente el acceso a la consola serie
- Utilizar etiquetas de recursos para controlar el acceso a la consola serie

Permitir explícitamente el acceso a la consola serie

De forma predeterminada, nadie tiene acceso a la consola serie. Para conceder acceso a la consola serie, debe configurar una política para permitir explícitamente el acceso. Se recomienda configurar una política que restrinja el acceso a instancias específicas.

La siguiente política permite el acceso a la consola serie de una instancia específica, identificada por su ID de instancia.

Tenga en cuenta que las acciones `DescribeInstances`, `DescribeInstanceTypes` y `GetSerialConsoleAccessStatus` no admiten permisos a nivel de recurso y, por lo tanto, todos los recursos, indicados por el `*` (asterisco), deben especificarse para estas acciones.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowDescribeInstances",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
```

```
                "ec2:DescribeInstanceTypes",
                "ec2:GetSerialConsoleAccessStatus"
            ],
             "Resource": "*"
        },
        {
            "Sid": "AllowinstanceBasedSerialConsoleAccess",
            "Effect": "Allow",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey"
            ],
            "Resource": "arn:aws:ec2:region:account-id:instance/i-0598c7d356eba48d7"
        }
    ]
}
```

Denegar explícitamente el acceso a la consola serie

La siguiente política de IAM permite el acceso a la consola serie de todas las instancias, indicada por el * (asterisco), y deniega explícitamente el acceso a la consola serie de una instancia específica, identificada por su ID.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSerialConsoleAccess",
            "Effect": "Allow",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:GetSerialConsoleAccessStatus"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DenySerialConsoleAccess",
            "Effect": "Deny",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey"
            ],
            "Resource": "arn:aws:ec2:region:account-id:instance/i-0598c7d356eba48d7"
```

```
        }
    ]
}
```

Utilizar etiquetas de recursos para controlar el acceso a la consola serie

Puede utilizar etiquetas de recursos para controlar el acceso a la consola serie de una instancia.

El control de acceso basado en atributos es una estrategia de autorización que define permisos basados en etiquetas que pueden asociarse a usuarios y recursos de AWS. Por ejemplo, la siguiente política permite a un usuario iniciar una conexión de consola serie para una instancia solo si la etiqueta de recurso de esa instancia y la etiqueta principal tienen el mismo valor `SerialConsole` para la clave de etiqueta.

Para obtener más información sobre el uso de etiquetas para controlar el acceso a los recursos de AWS, consulte Control de acceso a los recursos de AWS en la Guía del usuario de IAM.

Tenga en cuenta que las acciones `DescribeInstances`, `DescribeInstanceTypes` y `GetSerialConsoleAccessStatus` no admiten permisos a nivel de recurso y, por lo tanto, todos los recursos, indicados por el `*` (asterisco), deben especificarse para estas acciones.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowDescribeInstances",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:GetSerialConsoleAccessStatus"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowTagBasedSerialConsoleAccess",
            "Effect": "Allow",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey"
            ],
            "Resource": "arn:aws:ec2:region:account-id:instance/*",
            "Condition": {
```

```
                "StringEquals": {
                    "aws:ResourceTag/SerialConsole":
 "${aws:PrincipalTag/SerialConsole}"
                }
            }
        }
    ]
}
```

Cómo establecer una contraseña de usuario de SO en una instancia de Linux

> **Note**
>
> Esta sección se aplica únicamente a las instancias de Linux.

Puede conectarse a la consola serie sin una contraseña. Sin embargo, para utilizar la consola serie para solucionar problemas de una instancia de Linux, esta debe tener un usuario de sistema operativo basado en contraseña.

Puede establecer la contraseña para cualquier usuario del sistema operativo, incluido el usuario raíz. Tenga en cuenta que el usuario raíz puede modificar todos los archivos, mientras que cada usuario del sistema operativo puede tener permisos limitados.

Debe establecer una contraseña de usuario para cada instancia para la que vaya a utilizar la consola serie. Es un requisito de una sola vez para cada instancia.

> **Note**
>
> Las siguientes instrucciones solo son aplicables si ha lanzado la instancia mediante una AMI de Linux proporcionada por AWS porque, de forma predeterminada, las AMI proporcionadas por AWS no están configuradas con un usuario basado en contraseña. Si ha iniciado la instancia con una AMI que ya tiene configurada la contraseña de usuario raíz, puede omitir estas instrucciones.

Para establecer una contraseña de usuario de SO en una instancia de Linux

1. Conéctese a la instancia. Puede utilizar cualquier método para conectarse a la instancia, excepto el método de conexión de la consola serie de EC2.

2. Para establecer la contraseña de un usuario, utilice el comando passwd. En el siguiente ejemplo, el usuario es `root`.

```
[ec2-user ~]$ sudo passwd root
```

A continuación, se muestra un ejemplo del resultado.

```
Changing password for user root.
New password:
```

3. En la solicitud `New password`, ingrese la nueva contraseña.
4. En la solicitud, vuelva a ingresar la contraseña.

Conectar a la consola serie de EC2

Puede conectarse a la consola serie de su instancia de EC2 mediante la consola de Amazon EC2 o mediante SSH. Después de conectarse a la consola serie, puede usarla para solucionar problemas de arranque, configuración de red y otros problemas. Para obtener más información acerca de la solución de problemas, consulte Solución de problemas de la instancia de Amazon EC2 mediante la consola serie de EC2.

Consideraciones

- Solo se admite una conexión de consola serie activa por instancia.
- La conexión de la consola serie suele durar una hora a menos que se desconecte de ella. Sin embargo, durante el mantenimiento del sistema, Amazon EC2 desconectará la sesión de la consola serie.
- Se tardan 30 segundos en desconectar una sesión después de que se haya desconectado de la consola serie para permitir una nueva sesión.
- Puertos de consola serie compatibles: `ttyS0` (instancias de Linux) y `COM1` (instancias de Windows)
- Cuando se conecta a la consola serie, es posible que observe una ligera disminución en el rendimiento de la instancia.

Temas

- Conéctese utilizando el cliente basado en navegador

- Conexión con su propia clave y cliente SSH
- Puntos de conexión y huellas digitales de la consola serie de EC2

Conéctese utilizando el cliente basado en navegador

Puede conectarse a la consola serie de la instancia de EC2 mediante el cliente basado en navegador. Para ello, seleccione la instancia en la consola Amazon EC2 y elija conectarse a la consola serie. El cliente basado en explorador controla los permisos y proporciona una conexión correcta.

La consola serie de EC2 funciona desde la mayoría de los navegadores y admite la entrada de teclado y ratón.

Antes de utilizar la , compruebe que cumple los requisitos previos indicados en .

Para conectarse al puerto serie de la instancia mediante el cliente basado en explorador (consola de Amazon EC2)

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancia[s]).
3. Seleccione la instancia y elija Actions (Acciones), Monitor and troubleshoot (Supervisar y solucionar problemas), EC2 Serial Console (Consola serie de EC2), Connect (Conectar).

   También puede seleccionar la instancia y elegir Connect (Conectar), EC2 Serial Console (Consola serie de EC2), Connect (Conectar).

   Se abrirá una ventana de terminal en el navegador.
4. Pulse Intro. Si devuelve un mensaje de inicio de sesión, está conectado a la consola serie.

   Si la pantalla permanece negra, puede utilizar la siguiente información para ayudar a resolver problemas relacionados con la conexión a la consola serie:

   - Compruebe que ha configurado el acceso a la consola serie. Para obtener más información, consulte Configurar el acceso a la consola serie de EC2.
   - (Solo instancias de Linux) Utilice SysRq para conectarse a la consola serie. SysRq no requiere que se conecte a través del cliente basado en navegador. Para obtener más información, consulte Solucionar problemas de su instancia de Linux mediante SysRq.

- (Solo instancias de Linux) Reinicie getty. Si tiene acceso SSH a la instancia, conéctese a la instancia mediante SSH y reinicie getty utilizando el siguiente comando.

```
[ec2-user ~]$ sudo systemctl restart serial-getty@ttyS0
```

- Reinicie su instancia. Puede reiniciar la instancia mediante SysRq (instancias de Linux), la consola de EC2 o la AWS CLI. Para obtener más información, consulte Solucionar problemas de su instancia de Linux mediante SysRq (instancias de Linux) o Reinicio de su instancia.

5. (Solo instancias de Linux) En la solicitud `login`, escriba el nombre de usuario del usuario basado en contraseña que configuró anteriormente y, a continuación, presione Entrar.
6. (Solo instancias de Linux) En la solicitud `Password`, escriba la contraseña y, a continuación, presione Entrar.

Ahora ha iniciado sesión en la instancia y puede utilizar la consola serie para solucionar problemas.

Conexión con su propia clave y cliente SSH

Puede usar su propia clave SSH y conectarse a su instancia desde el cliente SSH que elija al utilizar la API de consola serie. Esto le permite aprovechar la capacidad de la consola serie de insertar una clave pública en la instancia.

Antes de conectarse, asegúrese de haber completado los requisitos previos.

Para conectarse a la consola serie de una instancia mediante SSH

1. Empuje la clave pública SSH a la instancia para iniciar una sesión de consola serie

   Use el comando send-serial-consola-ssh-public-key para insertar la clave pública SSH en la instancia. Esto inicia una sesión de consola serie.

   Si ya se ha iniciado una sesión de consola serie para esta instancia, el comando falla porque solo puede tener una sesión abierta a la vez. Se tardan 30 segundos en desconectar una sesión después de que se haya desconectado de la consola serie para permitir una nueva sesión.

```
aws ec2-instance-connect send-serial-console-ssh-public-key \
    --instance-id i-001234a4bf70dec41EXAMPLE \
    --serial-port 0 \
    --ssh-public-key file://my_key.pub \
    --region us-east-1
```

2. Conéctese a la consola serie con su clave privada

   Utilice el comando ssh para conectarse a la consola serie antes de quitar la clave pública del servicio de consola serie. Tiene 60 segundos antes de que se elimine.

   Utilice la clave privada que corresponda a la clave pública.

   El formato del nombre de usuario es `instance-id.port0`, que comprende el ID de instancia y el puerto 0. En el ejemplo siguiente, el nombre de usuario es `i-001234a4bf70dec41EXAMPLE.port0`.

   El punto de conexión del servicio de consola serie es diferente para cada región. Consulte la tabla Puntos de conexión y huellas digitales de la consola serie de EC2 correspondiente al punto de conexión de cada región. En el siguiente ejemplo, el servicio de consola serie se encuentra en la región *us-east-1*.

   ```
   ssh -i my_key i-001234a4bf70dec41EXAMPLE.port0@serial-console.ec2-instance-connect.us-east-1.aws
   ```

3. (Opcional) Verifique la huella digital

   Cuando se conecta por primera vez a la consola serie, se le pedirá que verifique la huella digital. Puede comparar la huella digital de la consola serie con la huella digital que se muestra para la verificación. Si estas huellas digitales no coinciden, alguien podría intentar un ataque man-in-the-middle (MITM). Si coinciden, puede conectarse con confianza a la consola serie.

   La siguiente huella digital es para el servicio de consola serie en la región us-east-1. Para ver las huellas dactilares de cada región, consulte Puntos de conexión y huellas digitales de la consola serie de EC2.

   ```
   SHA256:dXwn5ma/xadVMeBZGEru5l2gx+yI5LDiJaLUcz0FMmw
   ```

   > **Note**
   >
   > La huella digital solo aparece la primera vez que se conecta a la consola serie.

4. Pulse Intro. Si se devuelve un mensaje, está conectado a la consola serie.

   Si la pantalla permanece negra, puede utilizar la siguiente información para ayudar a resolver problemas relacionados con la conexión a la consola serie:

- Compruebe que ha configurado el acceso a la consola serie. Para obtener más información, consulte Configurar el acceso a la consola serie de EC2.
- (Solo instancias de Linux) Utilice SysRq para conectarse a la consola serie. SysRq no requiere que se conecte a través de SSH. Para obtener más información, consulte Solucionar problemas de su instancia de Linux mediante SysRq.
- (Solo instancias de Linux) Reinicie getty. Si tiene acceso SSH a la instancia, conéctese a la instancia mediante SSH y reinicie getty utilizando el siguiente comando.

```
[ec2-user ~]$ sudo systemctl restart serial-getty@ttyS0
```

- Reinicie su instancia. Puede reiniciar la instancia mediante SysRq (solo instancias de Linux), la consola de EC2 o la AWS CLI. Para obtener más información, consulte Solucionar problemas de su instancia de Linux mediante SysRq (solo instancias de Linux) o Reinicio de su instancia.

5. (Solo instancias de Linux) En la solicitud `login`, escriba el nombre de usuario del usuario basado en contraseña que configuró anteriormente y, a continuación, presione Entrar.
6. (Solo instancias de Linux) En la solicitud `Password`, escriba la contraseña y, a continuación, presione Entrar.

Ahora ha iniciado sesión en la instancia y puede utilizar la consola serie para solucionar problemas.

Puntos de conexión y huellas digitales de la consola serie de EC2

A continuación, se muestran los puntos de conexión de servicio y las huellas digitales de la consola serie de EC2. Para conectarse mediante programación a la consola serie de una instancia, se utiliza un punto de conexión de la consola serie de EC2. Las huellas digitales y los puntos de conexión de la consola serie de EC2 son únicos para cada región de AWS.

Nombre de la región	Región	Punto de conexión	Huella digital
Este de EE. UU. (Ohio)	us-east-2	serial-console.ec2-instance-connect.us-east-2.aws	SHA256:EhwPkTzRtTY7TRSzz26XbB0/HvV9jRM7mCZN0xw/d/0

Nombre de la región	Región	Punto de conexión	Huella digital
Este de EE. UU. (Norte de Virginia)	us-east-1	serial-console.ec2-instance-connect.us-east-1.aws	SHA256:dXwn5ma/xadVMeBZGEru5l2gx+yI5LDiJaLUcz0FMmw
Oeste de EE. UU. (Norte de California)	us-west-1	serial-console.ec2-instance-connect.us-west-1.aws	SHA256:OHldlcMET8u7QLSX3jmRTRAPFHVtqbyoLZBMUCqiH3Y
Oeste de EE. UU. (Oregón)	us-west-2	serial-console.ec2-instance-connect.us-west-2.aws	SHA256:EMCIe23TqKaBI6yGHainqZcMwqNkDhhAVHa1O2JxVUc
África (Ciudad del Cabo)	af-south-1	ec2-serial-console.af-south-1.api.aws	SHA256:RMWWZ2fVePeJUqzjO5jL2KIgXsczoHlz21Ed00biiWI
Asia-Pacífico (Hong Kong)	ap-east-1	ec2-serial-console.ap-east-1.api.aws	SHA256:T0Q1lpiXxChoZHplnAkjbP7tkm2xXViC9bJFsjYnifk
Asia-Pacífico (Hyderabad)	ap-south-2	ec2-serial-console.ap-south-2.api.aws	SHA256:WJgPBSwV4/shN+OPITValoewAuYj15DVW845JEhDKRs
Asia-Pacífico (Yakarta)	ap-southeast-3	ec2-serial-console.ap-southeast-3.api.aws	SHA256:5ZwgrCh+lfns32XITqL/4O0zIfbx4bZgsYFqy3o8mIk

Nombre de la región	Región	Punto de conexión	Huella digital
Asia-Pacífico (Melbourne)	ap-southeast-4	ec2-serial-console.ap-southeast-4.api.aws	SHA256:Av aq27hFgLv jn5gTSShZ 0oV7h90p0 GG46wfOeT6ZJvM
Asia Pacífico (Mumbai)	ap-south-1	serial-console.ec2-instance-connect.ap-south-1.aws	SHA256:oB LXcYmklqH HEbliARxEgH8IsO51r ezTPiSM35BsU40
Asia Pacífico (Osaka)	ap-northeast-3	ec2-serial-console.ap-northeast-3.api.aws	SHA256:Am0/ jiBKBnBuFnHr9aXs gEV3G8Tu/ vVHFXE/3UcyjsQ
Asia Pacífico (Seúl)	ap-northeast-2	serial-console.ec2-instance-connect.ap-northeast-2.aws	SHA256:FoqWXNX +DZ++GuNTztg9 PK49WYMqBX +FrcZM2dSrqrI
Asia Pacífico (Singapur)	ap-southeast-1	serial-console.ec2-instance-connect.ap-southeast-1.aws	SHA256:PL FNn7WnCQD Hx3qmwLu1Gy/ O8TUX7LQgZuaC6L 45CoY
Asia Pacífico (Sídney)	ap-southeast-2	serial-console.ec2-instance-connect.ap-southeast-2.aws	SHA256:yF vMwUK9lEU QjQTRoXXzuN+cW9/ VSe9W984Cf5Tgzo4

Nombre de la región	Región	Punto de conexión	Huella digital
Asia Pacífico (Tokio)	ap-northeast-1	serial-console.ec2-instance-connect.ap-northeast-1.aws	SHA256:RQfsDCZTOfQawewTRDV1t9Em/HMrFQe+CRlIOT5um4k
Canadá (Central)	ca-central-1	serial-console.ec2-instance-connect.ca-central-1.aws	SHA256:P2O2jOZwmpMwkpO6YW738FIOTHdUTyEv2gczYMMO7s4
China (Pekín)	cn-north-1	ec2-serial-console.cn-north-1.api.amazonwebservices.com.cn	SHA256:2gHVFy4H7uU3+WaFUxD28v/ggMeqjvSlgngpgLgGT+Y
China (Ningxia)	cn-northwest-1	ec2-serial-console.cn-northwest-1.api.amazonwebservices.com.cn	SHA256:TdgrNZkiQOdVfYEBUhO4SzUA09VWI5rYOZGTogpwmiM
Europa (Frankfurt)	eu-central-1	serial-console.ec2-instance-connect.eu-central-1.aws	SHA256:aCMFS/yIcOdOlkXvOl8AmZ1Toe+bBnrJJ3Fy0k0De2c
Europa (Irlanda)	eu-west-1	serial-console.ec2-instance-connect.eu-west-1.aws	SHA256:h2AaGAWO4Hathhtm6ezs3Bj7udgUxi2qTrHjZAwCW6E

Nombre de la región	Región	Punto de conexión	Huella digital
Europa (Londres)	eu-west-2	serial-console.ec2-instance-connect.eu-west-2.aws	SHA256:a69rd5CE/AEG4Amm53I6lkD1ZPvS/BCV3tTPW2RnJg8
Europa (Milán)	eu-south-1	ec2-serial-console.eu-south-1.api.aws	SHA256:lC0kOVJnpgFyBVrxn0A7n99ecLbXSX95cuuS7X7QK30
Europa (París)	eu-west-3	serial-console.ec2-instance-connect.eu-west-3.aws	SHA256:q8ldnAf9pymeNe8BnFVngY3RPAr/kxswJUzfrlxeEWs
Europa (España)	eu-south-2	ec2-serial-console.eu-south-2.api.aws	SHA256:GoCW2DFRlu669QNxqFxEcsR6fZUz/4F4n7T45ZcwoEc
Europa (Estocolmo)	eu-north-1	serial-console.ec2-instance-connect.eu-north-1.aws	SHA256:tkGFFUVUDvocDiGSS3Cu8Gdl6w2uI32EPNpKFKLwX84
Europa (Zúrich)	eu-central-2	ec2-serial-console.eu-central-2.api.aws	SHA256:8Ppx2mBMf6WdCw0NUlzKfwM4/lfRz4OaXFutQXWp6mk

Nombre de la región	Región	Punto de conexión	Huella digital
Israel (Tel Aviv)	il-central-1	ec2-serial-console.il-central-1.api.aws	SHA256:JR 6q8v6kNNP i8+QSFQ4d j5dimNmZP TgwgsM1SNvtYyU
Medio Oriente (Baréin)	me-south-1	ec2-serial-console .me-south-1.api.aws	SHA256:nP jLLKHu2Qn LdUq2kVAr soK5xvPJO MRJKCBzCDqC3k8
Medio Oriente (EAU)	me-central-1	ec2-serial-console .me-central-1.api.aws	SHA256:zpb5duKiBZ +l0dFwPeyy kB4MPBYhI/ XzXNeFSDKBvLE
América del Sur (São Paulo)	sa-east-1	serial-console.ec2-instance-connect.sa-east-1.aws	SHA256:rd2+/32Ognj ew1yVIemENaQzC +Botbih62OqAPDq1dI
AWS GovCloud (Este de EE. UU.)	us-gov-east-1	serial-console.ec2 -instance-connect. us-gov-east-1.amaz onaws.com	SHA256:tI we19GWsoy LClrtvu38YEEh+DHIk qnDcZnmtebvF28
AWS GovCloud (Oeste de EE.UU.)	us-gov-west-1	serial-console.ec2 -instance-connect. us-gov-west-1.amaz onaws.com	SHA256:kf OFRWLaOZfB +utbd3bRf8OlPf8nG O2YZLqXZiIw5DQ

Desconexión de la consola serie de EC2

Si ya no necesita estar conectado a la consola serie de EC2 de su instancia, puede desconectarse de ella. Al desconectarse de la consola serie, cualquier sesión de intérprete de comandos que se

ejecute en la instancia seguirá ejecutándose. Si quiere finalizar la sesión de intérprete de comandos, tendrá que finalizarla antes de desconectarse de la consola serie.

Consideraciones

- La conexión de la consola serie suele durar una hora a menos que se desconecte de ella. Sin embargo, durante el mantenimiento del sistema, Amazon EC2 desconectará la sesión de la consola serie.
- Se tardan 30 segundos en desconectar una sesión después de que se haya desconectado de la consola serie para permitir una nueva sesión.

La forma de desconectarse de la consola serie depende del cliente.

Cliente basado en explorador

Para finalizar la sesión de la consola serie, cierre la ventana del terminal del navegador de la consola serie.

Cliente OpenSSH estándar

Para desconectarse de la consola serie, utilice el siguiente comando para cerrar la conexión SSH. Este comando debe ejecutarse inmediatamente después de una nueva línea.

```
~.
```

El comando que se utiliza para cerrar una conexión SSH puede ser diferente dependiendo del cliente SSH que esté utilizando.

Solución de problemas de la instancia de Amazon EC2 mediante la consola serie de EC2

Mediante la consola serie de EC2, puede solucionar problemas de arranque, configuración de red y otros problemas conectándose al puerto serie de la instancia.

> **Note**
>
> Antes de comenzar, compruebe que cumple los requisitos previos.

instancias de Linux

Temas

- Solucionar problemas de su instancia de Linux mediante GRUB
- Solucionar problemas de su instancia de Linux mediante SysRq

Solucionar problemas de su instancia de Linux mediante GRUB

GNU GRUB (abreviatura de GNU Grand Unified Bootloader, comúnmente conocido como GRUB) es el gestor de arranque predeterminado para la mayoría de los sistemas operativos Linux. Desde el menú GRUB, puede seleccionar en qué núcleo desea arrancar, o modificar las entradas del menú para cambiar la forma en que arrancará el kernel. Esto puede ser útil cuando se solucionan problemas en una instancia que falla.

El menú GRUB se muestra durante el proceso de arranque. No se puede acceder al menú a través de SSH normal, pero se puede acceder a él a través de la consola serie de EC2.

Single user mode

El modo de usuario único iniciará el kernel en un nivel de ejecución inferior. Por ejemplo, podría montar el sistema de archivos pero no activar la red, dándole la oportunidad de realizar el mantenimiento necesario para corregir la instancia.

Para arrancar en modo de usuario único

1. Conéctese a la consola serie de la instancia.
2. Ejecute el siguiente comando para volver a arrancar la instancia.

```
[ec2-user ~]$ sudo reboot
```

3. Durante el reinicio, cuando aparezca el menú GRUB, pulse cualquier tecla para detener el proceso de arranque.
4. En el menú GRUB, utilice las teclas de flecha para seleccionar el núcleo en el que se va a arrancar y presione e el teclado.
5. Utilice las teclas de dirección para localizar el cursor en la línea que contiene el núcleo. La línea comienza con `linux` o `linux16` en función de la AMI que se utilizó para iniciar la instancia. Para Ubuntu, comienzan con dos líneas `linux`, que deben modificarse en el siguiente paso.

6. Al final de la línea, agregue la palabra `single`.

   A continuación se muestra un ejemplo de Amazon Linux 2.

   ```
   linux /boot/vmlinuz-4.14.193-149.317.amzn2.aarch64 root=UUID=d33f9c9a-\
   dadd-4499-938d-ebbf42c3e499 ro  console=tty0 console=ttyS0,115200n8 net.ifname\
   s=0 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff rd.she\
   ll=0 single
   ```

7. Presione Ctrl+X para arrancar en modo de usuario único.
8. En la solicitud `login`, escriba el nombre de usuario del usuario basado en contraseña que configuró anteriormente y, a continuación, presione Enter (Entrar).
9. En la solicitud `Password`, escriba la contraseña y, a continuación, presione Enter (Entrar).

Emergency mode

El modo de emergencia es similar al modo de usuario único, excepto que el núcleo se ejecuta en el nivel de ejecución más bajo posible.

Para arrancar en modo de emergencia, siga los mismos pasos del modo de usuario único, pero en el paso 6 agregue la palabra `emergency` en lugar de `single`.

Solucionar problemas de su instancia de Linux mediante SysRq

La clave System Request (SysRq), que a veces se conoce como “magic SysRq”, se puede usar para enviar directamente al kernel un comando, fuera de un shell, y el kernel responderá, independientemente de lo que esté haciendo el kernel. Por ejemplo, si la instancia ha dejado de responder, puede usar la clave SysRq para indicar al kernel que se bloquee o se reinicie. Para obtener más información, consulte la tecla Magic SysRq en Wikipedia.

Puede utilizar comandos SysRq en el cliente basado en el explorador de la consola serie de EC2 o en un cliente SSH. El comando para enviar una solicitud de interrupción es diferente para cada cliente.

Para utilizar SysRq, elija uno de los procedimientos siguientes según el cliente que esté utilizando.

Browser-based client

Para utilizar SysRq en el cliente basado en explorador de consola serie

1. Conéctese a la consola serie de la instancia.
2. Para enviar una solicitud de interrupción, pulse `CTRL+0` (cero). Si el teclado lo admite, también puede enviar una solicitud de interrupción utilizando las teclas Pausa o Descanso.

```
[ec2-user ~]$ CTRL+0
```

3. Para ejecutar un comando SysRq, presione la tecla del teclado que corresponda al comando requerido. Por ejemplo, para mostrar una lista de comandos SysRq, presione h.

```
[ec2-user ~]$ h
```

El h comando genera algo similar al siguiente.

```
[ 1169.389495] sysrq: HELP : loglevel(0-9) reboot(b) crash(c) terminate-all-
tasks(e) memory-full-oom-kill(f) kill-all-tasks(i) thaw-filesystems
(j) sak(k) show-backtrace-all-active-cpus(l) show-memory-usage(m) nice-all-RT-
tasks(n) poweroff(o) show-registers(p) show-all-timers(q) unraw(r
) sync(s) show-task-states(t) unmount(u) show-blocked-tasks(w) dump-ftrace-
buffer(z)
```

SSH client

Para usar SysRq en un cliente SSH

1. Conéctese a la consola serie de la instancia.
2. Para enviar una solicitud de interrupción, pulse `~B` (tilde, seguido de mayúsculas `B`).

```
[ec2-user ~]$ ~B
```

3. Para ejecutar un comando SysRq, presione la tecla del teclado que corresponda al comando requerido. Por ejemplo, para mostrar una lista de comandos SysRq, presione h.

```
[ec2-user ~]$ h
```

El h comando genera algo similar al siguiente.

```
[ 1169.389495] sysrq: HELP : loglevel(0-9) reboot(b) crash(c) terminate-all-
tasks(e) memory-full-oom-kill(f) kill-all-tasks(i) thaw-filesystems
(j) sak(k) show-backtrace-all-active-cpus(l) show-memory-usage(m) nice-all-RT-
tasks(n) poweroff(o) show-registers(p) show-all-timers(q) unraw(r
) sync(s) show-task-states(t) unmount(u) show-blocked-tasks(w) dump-ftrace-
buffer(z)
```

> **Note**
>
> El comando que utiliza para enviar una solicitud de interrupción puede ser diferente dependiendo del cliente SSH que esté utilizando.

instancias de Windows

Usar SAC para solucionar problemas de su instancia de Windows

La capacidad de la Consola de administración especial (SAC) de Windows proporciona una forma de solucionar problemas de una instancia de Windows. Al conectarse a la consola serie de la instancia y usar SAC, puede interrumpir el proceso de arranque e iniciar Windows en modo seguro.

> **Note**
>
> Si habilita SAC en una instancia, los servicios de EC2 que dependen de la recuperación de contraseñas no funcionarán desde la consola de Amazon EC2. Los agentes de lanzamiento de Windows en Amazon EC2 (EC2Config, EC2Launch v1 y EC2Launch v2) dependen de la consola serie para ejecutar diversas tareas. Esas tareas no se ejecutan correctamente cuando se habilita SAC en una instancia. Para obtener más información sobre los agentes de lanzamiento de Windows en Amazon EC2, consulte the section called “Configuración de instancias de Windows”. Si habilita SAC, podrá desactivarlo más adelante. Para obtener más información, consulte Desactivar SAC y el menú de inicio.

Temas

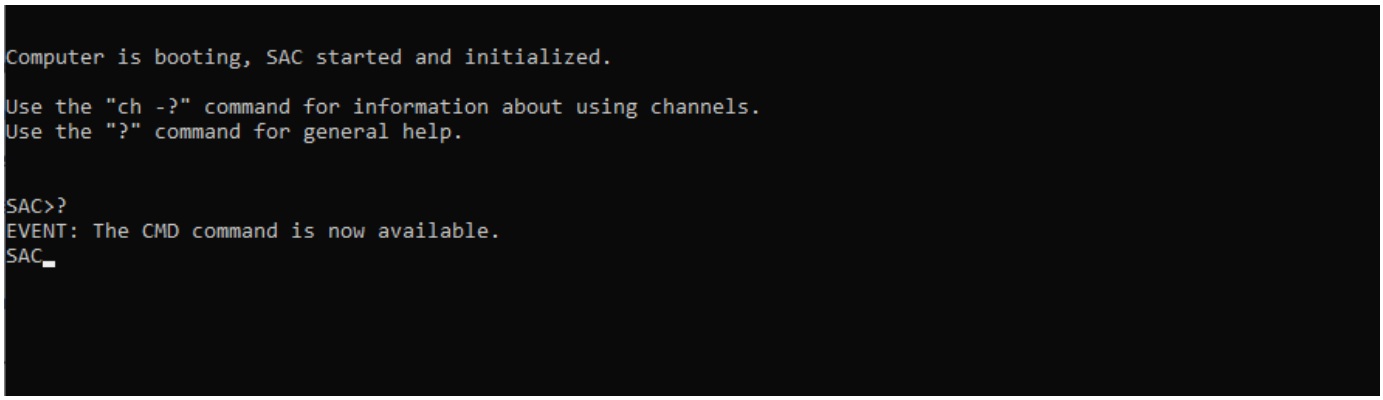
- Utilizar SAC
- Usar el menú de inicio
- Desactivar SAC y el menú de inicio

Utilizar SAC

Para utilizar SAC

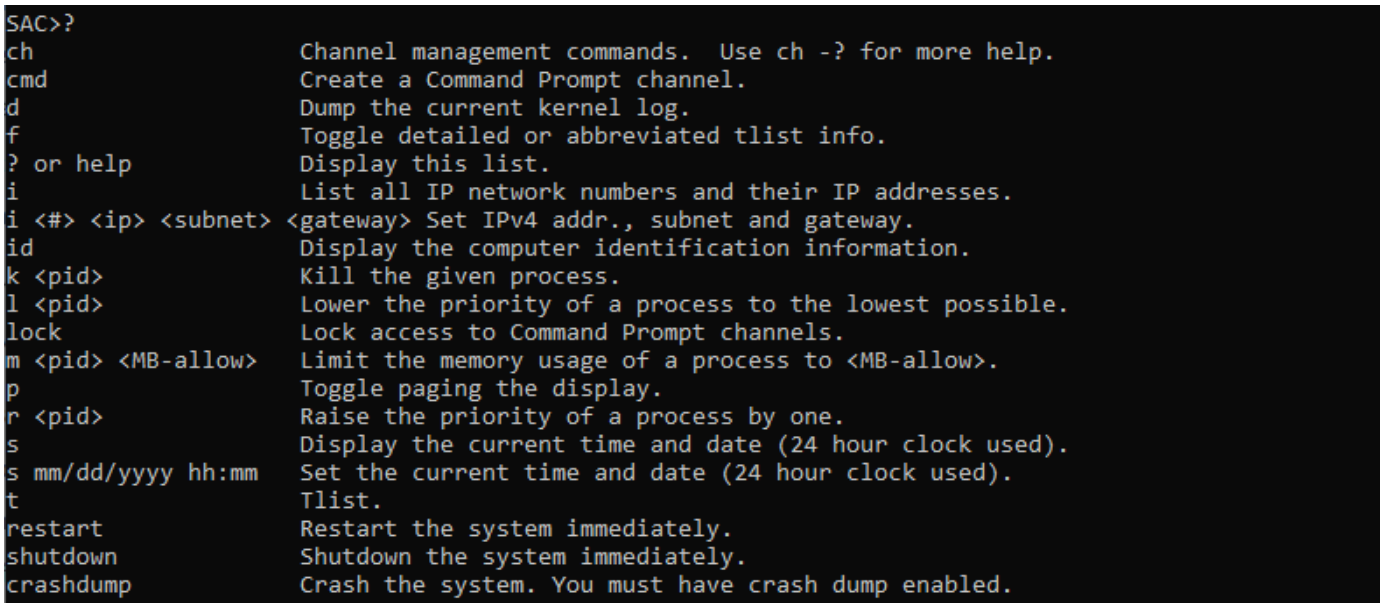
1. Conéctese a la consola serie.

   Si SAC se ha habilitado en la instancia, la consola serial muestra el mensaje `SAC>`.



2. Para mostrar los comandos SAC, ingrese **?** y, a continuación, pulse Enter (Intro).

   Resultado previsto



3. Para crear un canal de símbolo del sistema (como `cmd0001` o `cmd0002`), ingrese **`cmd`** y, a continuación, pulse Enter (Ingresar).
4. Para ver el canal del símbolo del sistema, pulse ESC y, a continuación, TAB.

   Resultado previsto

```
Name:                 Cmd0001
Description:          Command
Type:                 VT-UTF8
Channel GUID:         ef9f20a0-1287-11eb-82b0-0e4ba51872e5
Application Type GUID: 63d02271-8aa4-11d5-bccf-00b0d014a2d0

Press <esc><tab> for next channel.
Press <esc><tab>0 to return to the SAC channel.
Use any other key to view this channel.
```

5. Para cambiar de canal, pulse simultáneamente ESC+TAB+número de canal. Por ejemplo, para cambiar al canal `cmd0002` (si se ha creado), pulse ESC+TAB+2.
6. Escriba las credenciales requeridas por el canal del símbolo del sistema.

```
Please enter login credentials.
Username: Administrator
Domain  : .
Password: *******
```

El símbolo del sistema es el mismo intérprete de comandos con todas las funciones que obtiene en un escritorio, pero con la excepción de que no permite la lectura de caracteres que ya se produjeron.

```
Microsoft Windows [Version 10.0.17763.1457]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>diskpart

Microsoft DiskPart version 10.0.17763.1

Copyright (C) Microsoft Corporation.
On computer: EC2AMAZ-ASR4SAI

DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online           30 GB      0 B
  Disk 1    Online           46 GB    46 GB

DISKPART>
```

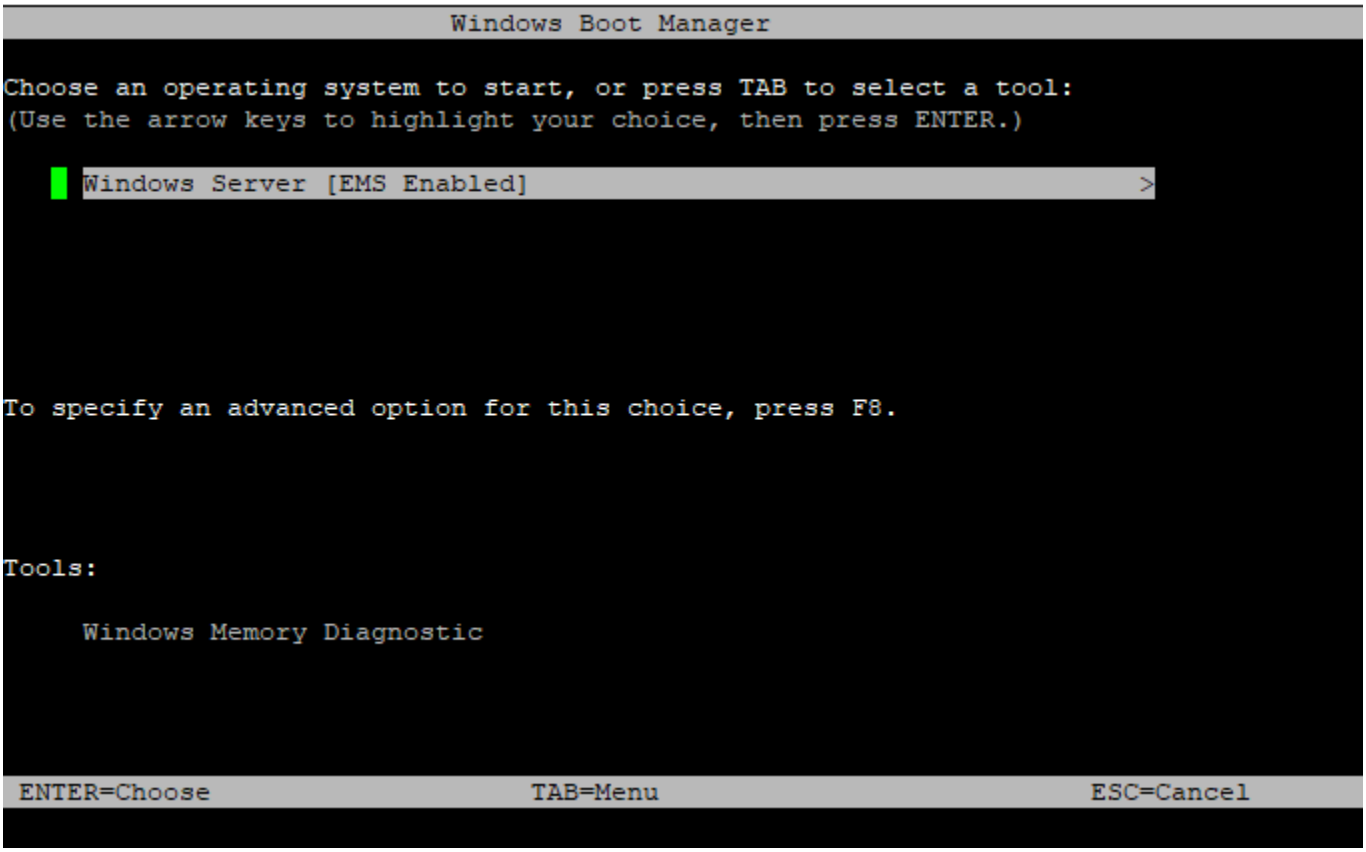
PowerShell también se puede utilizar desde el símbolo del sistema.

Tenga en cuenta que es posible que deba establecer la preferencia de progreso en modo silencioso.

```
PS C:\Windows\system32> $ProgressPreference="SilentlyContinue"
PS C:\Windows\system32> $computerInfo = Get-ComputerInfo
PS C:\Windows\system32> $computerInfo.Csprocessors[0].Name
Intel(R) Xeon(R) Platinum 8124M CPU @ 3.00GHz
PS C:\Windows\system32> $computerInfo.Csprocessors[0].Description
Intel64 Family 6 Model 85 Stepping 4
PS C:\Windows\system32>
```

Usar el menú de inicio

Si la instancia tiene habilitado el menú de inicio y se reinicia después de conectarse a través de SSH, debería ver el menú de arranque, como se indica a continuación.



Comandos del menú Reiniciar

ENTER (INTRO)

Inicia la entrada seleccionada del sistema operativo.

TAB

Cambia al menú Herramientas.

ESC

Cancela y reinicia la instancia.

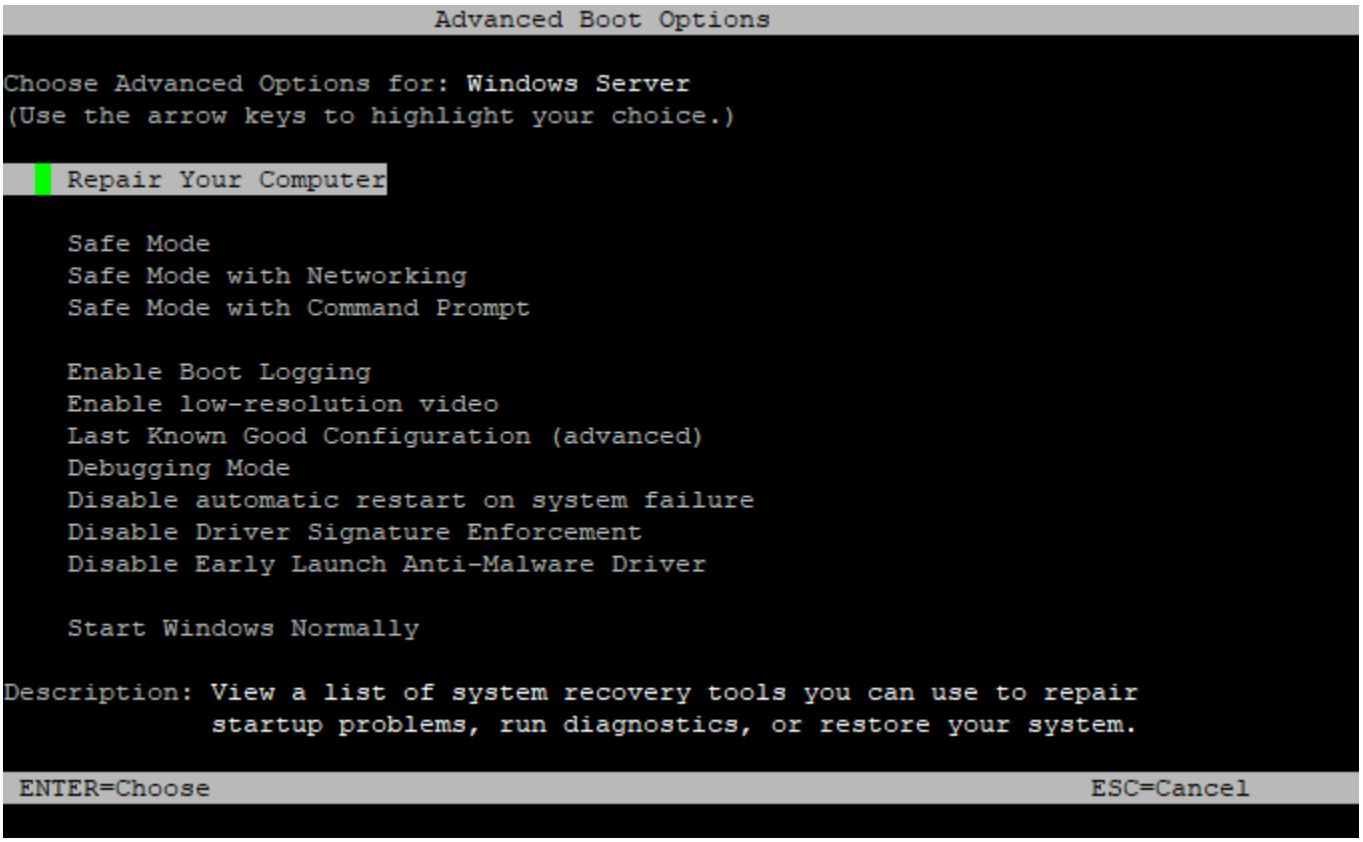
ESC seguido de 8

Equivalente a presionar F8. Muestra opciones avanzadas para el elemento seleccionado.

Tecla ESC + flecha izquierda

Vuelve al menú de inicio inicial.

> **Note**
>
> La tecla ESC por sí sola no lo lleva de vuelta al menú principal porque Windows está esperando a ver si hay una secuencia de escape en curso.



Desactivar SAC y el menú de inicio

Si habilita SAC y el menú de inicio, podrá desactivar estas funciones más adelante.

Utilice uno de los métodos siguientes para desactivar SAC y el menú de inicio en una instancia.

PowerShell

Para desactivar SAC y el menú de inicio en una instancia de Windows

1. Conéctese a la instancia y realice los siguientes pasos desde la línea de comandos elevada de PowerShell.
2. En primer lugar, desactive el menú de inicio cambiando el valor a `no`.

```
bcdedit /set '{bootmgr}' displaybootmenu no
```

3. A continuación, desactive SAC cambiando el valor a `off`.

```
bcdedit /ems '{current}' off
```

4. Aplique la configuración actualizada reiniciando la instancia.

```
shutdown -r -t 0
```

Command prompt

Para desactivar SAC y el menú de inicio en una instancia de Windows

1. Conéctese a la instancia y realice los siguientes pasos desde el símbolo del sistema.
2. En primer lugar, desactive el menú de inicio cambiando el valor a `no`.

```
bcdedit /set {bootmgr} displaybootmenu no
```

3. A continuación, desactive SAC cambiando el valor a `off`.

```
bcdedit /ems {current} off
```

4. Aplique la configuración actualizada reiniciando la instancia.

```
shutdown -r -t 0
```

Enviar una interrupción de diagnóstico (usuarios avanzados)

> **Warning**
>
> Las interrupciones de diagnóstico están destinadas a ser utilizadas por usuarios avanzados. El uso incorrecto podría afectar negativamente a su instancia. El envío de una interrupción de diagnóstico a una instancia podría desencadenar que una instancia se bloquee y reinicie, lo que podría provocar la pérdida de datos.

Puede enviar una interrupción de diagnóstico a una instancia inaccesible o que no responde para activar un pánico de kernel (en instancias de Linux) o un error de parada (denominado comúnmente error de pantalla azul) en instancias de Windows.

instancias de Linux

Los sistemas operativos Linux normalmente se bloquean y se reinician cuando se produce un pánico de kernel. El comportamiento específico del sistema operativo depende de su configuración. Un pánico de kernel también se puede utilizar para hacer que el kernel del sistema operativo de la instancia realice tareas como, por ejemplo, generar un archivo de volcado de bloqueo. A continuación, puede utilizar la información del archivo de volcado de bloqueo para realizar un análisis de causa raíz y depurar la instancia. El sistema operativo genera los datos de volcado de memoria localmente en la propia instancia.

instancias de Windows

En general, los sistemas operativos Windows se bloquean y reinician cuando se produce un error de parada, pero el comportamiento específico depende de su configuración. Un error de parada también puede hacer que el sistema operativo escriba información de depuración de errores como, por ejemplo, un volcado de memoria de kernel, en un archivo. A continuación, puede utilizar esta información para llevar a cabo un análisis de causa raíz para depurar la instancia. El sistema operativo genera los datos de volcado de memoria localmente en la propia instancia.

Antes de enviar una interrupción de diagnóstico a la instancia, le recomendamos que consulte la documentación del sistema operativo y, a continuación, realice los cambios de configuración necesarios.

Contenido

Tipos de instancias admitidas

La interrupción de diagnóstico es compatible con todos los tipos de instancias basadas en Nitro, a excepción de los que funcionan con procesadores Graviton de AWS. Para obtener más información, consulte las instancias integradas en el AWS Nitro System y AWS Graviton.

Requisitos previos

Antes de utilizar una interrupción de diagnóstico, debe configurar el sistema operativo de la instancia. Esto garantiza que realice las acciones que necesita cuando se produce un pánico de kernel (instancias de Linux) o un error de parada (instancias de Windows).

instancias de Linux

Para configurar Amazon Linux 2 para generar un volcado de bloqueo cuando se produce un pánico de kernel

1. Conéctese a la instancia.
2. Instale kexec y kdump.

```
[ec2-user ~]$ sudo yum install kexec-tools -y
```

3. Configure el kernel para reservar una cantidad de memoria adecuada para el kernel secundario. La cantidad de memoria que reservar depende de la memoria total disponible de la instancia. Abra el archivo `/etc/default/grub` utilizando su editor de texto preferido, localice la línea que comienza por `GRUB_CMDLINE_LINUX_DEFAULT` y, a continuación, añada el parámetro `crashkernel` con el formato siguiente: `crashkernel=`*`memory_to_reserve`*. Por ejemplo, para reservar `160MB`, modifique el archivo `grub` como se indica a continuación:

```
GRUB_CMDLINE_LINUX_DEFAULT="crashkernel=160M console=tty0 console=ttyS0,115200n8
 net.ifnames=0 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff
 rd.shell=0"
GRUB_TIMEOUT=0
GRUB_DISABLE_RECOVERY="true"
```

4. Guarde los cambios y cierre el archivo `grub`.

5. Vuelva a compilar el archivo de configuración GRUB2.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

6. En instancias basadas en procesadores Intel y AMD, el comando `send-diagnostic-interrupt` envía una interrupción no enmascarable desconocida (NMI) a la instancia. Debe configurar el kernel para que se bloquee cuando reciba la NMI desconocida. Abra el archivo `/etc/sysctl.conf` con su editor de texto preferido y agregue lo siguiente.

```
kernel.unknown_nmi_panic=1
```

7. Reinicie la instancia y vuelva a conectarse a ella.
8. Compruebe que el kernel se haya iniciado con el parámetro `crashkernel` correcto.

```
$ grep crashkernel /proc/cmdline
```

   La siguiente salida de ejemplo indica una configuración correcta.

```
BOOT_IMAGE=/boot/vmlinuz-4.14.128-112.105.amzn2.x86_64 root=UUID=a1e1011e-
e38f-408e-878b-fed395b47ad6 ro crashkernel=160M console=tty0 console=ttyS0,115200n8
 net.ifnames=0 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff
 rd.shell=0
```

9. Compruebe que el servicio kdump está en ejecución.

```
[ec2-user ~]$ systemctl status kdump.service
```

   La siguiente salida de ejemplo muestra el resultado si el servicio kdump se está ejecutando.

```
kdump.service - Crash recovery kernel arming
   Loaded: loaded (/usr/lib/systemd/system/kdump.service; enabled; vendor preset:
 enabled)
   Active: active (exited) since Fri 2019-05-24 23:29:13 UTC; 22s ago
  Process: 2503 ExecStart=/usr/bin/kdumpctl start (code=exited, status=0/SUCCESS)
 Main PID: 2503 (code=exited, status=0/SUCCESS)
```

> **Note**
>
> De forma predeterminada, el archivo de volcado de bloque se guarda en `/var/crash/`. Para cambiar la ubicación, modifique el archivo `/etc/kdump.conf` utilizando su editor de texto preferido.

Para configurar Amazon Linux para generar un volcado de bloqueo cuando se produce un pánico de kernel

1. Conéctese a la instancia.
2. Instale kexec y kdump.

   ```
   [ec2-user ~]$ sudo yum install kexec-tools -y
   ```

3. Configure el kernel para reservar una cantidad de memoria adecuada para el kernel secundario. La cantidad de memoria que reservar depende de la memoria total disponible de la instancia.

   ```
   $ sudo grubby --args="crashkernel=memory_to_reserve" --update-kernel=ALL
   ```

   Por ejemplo, para reservar `160MB` para el kernel de bloqueo, utilice el comando siguiente.

   ```
   $ sudo grubby --args="crashkernel=160M" --update-kernel=ALL
   ```

4. En instancias basadas en procesadores Intel y AMD, el comando `send-diagnostic-interrupt` envía una interrupción no enmascarable desconocida (NMI) a la instancia. Debe configurar el kernel para que se bloquee cuando reciba la NMI desconocida. Abra el archivo `/etc/sysctl.conf` con su editor de texto preferido y agregue lo siguiente.

   ```
   kernel.unknown_nmi_panic=1
   ```

5. Reinicie la instancia y vuelva a conectarse a ella.
6. Compruebe que el kernel se haya iniciado con el parámetro `crashkernel` correcto.

   ```
   $ grep crashkernel /proc/cmdline
   ```

   La siguiente salida de ejemplo indica una configuración correcta.

```
root=LABEL=/ console=tty1 console=ttyS0 selinux=0 nvme_core.io_timeout=4294967295
 LANG=en_US.UTF-8 KEYTABLE=us crashkernel=160M
```

7. Compruebe que el servicio kdump está en ejecución.

```
[ec2-user ~]$ sudo service kdump status
```

Si el servicio se está ejecutando, el comando devuelve la respuesta `Kdump is operational`.

> **Note**
>
> De forma predeterminada, el archivo de volcado de bloque se guarda en `/var/crash/`. Para cambiar la ubicación, modifique el archivo `/etc/kdump.conf` utilizando su editor de texto preferido.

Para configurar SUSE Linux Enterprise, Ubuntu o Red Hat Enterprise Linux

En instancias basadas en procesadores Intel y AMD, el comando `send-diagnostic-interrupt` envía una interrupción no enmascarable desconocida (NMI) a la instancia. Debe configurar el kernel para que se bloquee cuando reciba la NMI desconocida, al ajustar el archivo de configuración del sistema operativo. Para obtener más información acerca de cómo configurar el kernel para que se bloquee, consulte la documentación de su sistema operativo:

- SUSE Linux Enterprise
- Ubuntu
- Red Hat Enterprise Linux (RHEL)

instancias de Windows

Para configurar Windows para generar un volcado de memoria cuando se produce un error de parada

1. Conéctese a la instancia.
2. Abra el Panel de control y seleccione Sistema, Configuración avanzada del sistema.
3. En el cuadro de diálogo Propiedades del sistema, seleccione la pestaña Avanzadas.

4. En la sección Inicio y recuperación, elija Configuración....
5. En la sección Error del sistema, establezca la configuración según sea necesario y, a continuación, elija Aceptar.

Para obtener más información sobre la configuración de errores de parada de Windows, consulte Overview of memory dump file options for Windows.

Enviar una interrupción de diagnóstico

Después de haber completado los cambios de configuración necesarios, puede enviar una interrupción de diagnóstico a su instancia mediante la AWS CLI o la API de Amazon EC2.

AWS CLI

Para enviar una interrupción de diagnóstico a su instancia (AWS CLI)

Utilice el comando send-diagnostic-interrupt y especifique el ID de instancia.

```
aws ec2 send-diagnostic-interrupt --instance-id i-1234567890abcdef0
```

PowerShell

Para enviar una interrupción de diagnóstico a su instancia (AWS Tools for Windows PowerShell)

Utilice el comando Send-EC2DiagnosticInterrupt y especifique el ID de instancia.

```
PS C:\> Send-EC2DiagnosticInterrupt -InstanceId i-1234567890abcdef0
```

Historial del documento

En la siguiente tabla se describen los cambios importantes de la Guía del usuario de Amazon EC2 a partir de 2019. Actualizamos la guía con frecuencia para dar respuesta a los comentarios que nos envía.

Cambio	Descripción	Fecha
Buscador de tipos de instancias EC2: parámetros adicionales	El buscador de tipos de instancias EC2 ahora proporciona parámetros adicionales para que pueda especificar los requisitos más detallados de su carga de trabajo.	5 de junio de 2024
Instancias U7i-12tb, U7in-16tb, U7in-24tb y U7in-32tb	Nuevos tipos de instancia de memoria elevada con procesadores escalables Intel Xeon de cuarta generación.	28 de mayo de 2024
Nueva política administrada para el lanzamiento rápido de EC2	Se agregó la política EC2FastLaunchFullAccess para realizar acciones de API relacionadas con la característica de lanzamiento rápido de EC2 desde una instancia.	14 de mayo de 2024
Protección contra la anulación del registro de la AMI	Puede activar la protección contra la anulación del registro en una AMI para evitar su eliminación accidental o malintencionada.	23 de abril de 2024

Reloj de equipo de PTP: soporte para tipos de instancias	El reloj de equipo de PTP ahora está disponible en los tipos de instancias C7a, C7i, M7a, M7g, M7i, R7a y R7i.	22 de abril de 2024
Adición de consideraciones de rendimiento de Nitro para mejorar las redes	Esta página se centra en las consideraciones de red para ayudar a ajustar el rendimiento de las instancias de Amazon EC2 basadas en Nitro.	4 de abril de 2024
Nueva política administrada para instantáneas de EBS compatibles con VSS	VSS de Amazon EC2 tiene disponible una nueva política administrada de IAM que puede añadir a su rol de perfil de instancia para garantizar que sus permisos estén actualizados y sigan las prácticas recomendadas.	28 de marzo de 2024
Reloj de equipo de PTP: Este de EE. UU. (Norte de Virginia)	El reloj de equipo de PTP ya está disponible en la región Este de EE. UU. (Norte de Virginia).	26 de marzo de 2024
Ajuste de IMDSv2 como valor predeterminado de cuenta	Puede configurar todos los inicializacións de instancias de EC2 nuevos en la cuenta para que usen el Servicio de metadatos de instancia, versión 2 (IMDSv2) de forma predeterminada.	25 de marzo de 2024
Etiquetado de las nuevas AMI de Linux creadas a partir de una instantánea	Al crear una AMI de Linux a partir de una instantánea, puede etiquetar la nueva AMI.	7 de marzo de 2024

Etiquetado de las nuevas AMI e instantáneas al copiarlas	Cuando copia una AMI, puede asignar etiquetas a la nueva AMI y las nuevas instantán eas con las mismas etiquetas o puede asignarles etiquetas diferentes.	7 de marzo de 2024
Eliminación de páginas de AWS Management Pack	AWS Management Pack se utilizó principalmente con Windows Server 2012 y versiones anteriores. Estas versiones heredadas de plataformas de sistemas operativos ya no son compatibles. Para administr ar la flota de servidores que se ejecutan en AWS y en las instalaciones y soluciona r problemas relacionados, consulte AWS Systems Manager Fleet Manager.	12 de febrero de 2024
EC2 Instance Connect preinstalado en las AMI de macOS	EC2 Instance Connect ahora viene preinstalado en las AMI de macOS Sonoma 14.2.1 o posterior, macOS Ventura 13.6.3 o posterior y macOS Monterey 12.7.2 o posterior.	26 de enero de 2024
Compatibilidad de EC2 Instance Connect con CentOS, macOS y RHEL	Ahora puede instalar EC2 Instance Connecct en las AMI de CentOS, macOS y RHEL compatibles.	6 de diciembre de 2023

Compatibilidad de la hibernación con C7a, C7i, R7a, R7i y R7iz	Hiberne las instancias recién iniciadas que se ejecutan en los tipos de instancias C7a, C7i, R7a, R7i y R7iz.	1 de diciembre de 2023
Selector de tipos de instancias de EC2 de Amazon Q	El selector de tipos de instancias de EC2 de Amazon Q tiene en cuenta su caso de uso, el tipo de carga de trabajo y las preferencias del fabricante de la CPU, así como la forma en que prioriza el precio y el rendimiento. A continuación, utiliza estos datos para proporcionar orientación y sugerencias sobre los tipos de instancias de Amazon EC2 que mejor se adapten a sus nuevas cargas de trabajo.	28 de noviembre de 2023
Nivel gratuito de EC2	Puede realizar un seguimiento del uso del nivel gratuito de EC2 desde el panel de EC2.	26 de noviembre de 2023

Console-to-Code	Console-to-Code puede ayudarlo a empezar a usar el código de automatización. Console-to-Code registra las acciones de la consola y, a continuación, utiliza la IA generativa para sugerir código en el formato de infraestructura como código que prefiera. Puede usar el código como punto de partida y personalizarlo para que esté listo para producción en función de su caso de uso específico.	26 de noviembre de 2023
Tiempos de espera configurables de seguimiento de conexiones inactivas	Las conexiones de grupos de seguridad que permanecen inactivas pueden provocar que se agote el seguimiento de las conexiones, que no se rastreen y que se pierdan paquetes. Ahora puede configurar el tiempo de espera, en segundos, para el seguimiento de conexiones de grupos de seguridad en una interfaz de red elástica.	17 de noviembre de 2023
Reloj de hardware de PTP	Las instancias compatibles ahora tienen un reloj de hardware del protocolo de tiempo preciso (PTP). El reloj de hardware de PTP admite una conexión NTP o una conexión PTP directa.	16 de noviembre de 2023

Cambio del tipo de instancia habilitada para la hibernación	Ahora puede cambiar el tipo de una instancia habilitada para la hibernación cuando se encuentra en estado `stopped`.	16 de noviembre de 2023
Topología de instancia	Puede usar la API DescribeInstanceTopology para detectar la ubicación de sus instancias y, luego, usar esta información para optimizar los trabajos de HPC y ML mediante su ejecución en instancias que estén físicamente más cerca unas de otras.	13 de noviembre de 2023
Compatibilidad con AMI compartidas de lanzamiento rápido de EC2	Ahora puede habilitar el lanzamiento rápido de EC2 en una AMI que se comparta con usted. Cuando habilita el lanzamiento rápido de EC2 en una AMI compartida, las instantáneas aprovisionadas previamente para un inicio más rápido se crean en su cuenta.	6 de noviembre de 2023
Bloques de capacidad para ML	Ahora puede reservar instancias de GPU para el futuro a fin de respaldar sus cargas de trabajo de machine learning (ML) de corta duración.	31 de octubre de 2023

Hibernación de instancias de spot	Ahora puede hibernar sus instancias de spot con la misma experiencia de hibernación y las mismas familias de instancias que están disponibles actualmente para las instancias bajo demanda.	24 de octubre de 2023
Configuración predeterminada del bloqueo del acceso público de las AMI	El bloqueo del acceso público de las AMI ahora está habilitado de forma predeterminada para todas las cuentas nuevas y para las cuentas existentes sin AMI públicas.	20 de octubre de 2023
Amazon EC2 Global View	Amazon EC2 Global View admite tipos de recursos adicionales y opciones de visualización personalizables.	18 de octubre de 2023
Compatibilidad con hibernación para Ubuntu 22.04.2 LTS (Jammy Jellyfish)	Hiberne las instancias recién iniciadas que se iniciaron desde la AMI de Ubuntu 22.04.2 LTS (Jammy Jellyfish).	16 de octubre de 2023
Deshabilitación de una AMI	Puede deshabilitar una AMI para evitar que se utilice en inicializacións de instancias.	12 de octubre de 2023
Comprobaciones de estado de EBS adjuntas	Puede utilizar las comprobaciones de estado de EBS adjuntas para supervisar si se puede acceder a los volúmenes de Amazon EBS adjuntos a una instancia.	11 de octubre de 2023

Soporte de hibernación para Red Hat Enterprise Linux 9	Hiberne las instancias recién iniciadas que se iniciaron desde AMI de Red Hat Enterprise Amazon Linux 9.	2 de octubre de 2023
Soporte de hibernación para Microsoft Windows Server 2022	Hiberne las instancias recién iniciadas que se iniciaron desde la AMI de Microsoft Windows Server 2022.	2 de octubre de 2023
Soporte de hibernación para AL2023	Hiberne las instancias recién iniciadas que se iniciaron desde la AMI de AL2023.	2 de octubre de 2023
Iniciar la interrupción de instancias de spot de una flota de spot	Puede seleccionar una flota de spot en la consola de Amazon EC2 e iniciar una interrupción de instancias de spot de la flota para probar cómo las aplicaciones de sus instancias de spot administran las interrupciones.	21 de septiembre de 2023
Bloqueo del acceso público de las AMI	Puede habilitar el bloqueo del acceso público de las AMI a nivel de cuenta para bloquear cualquier intento de hacerlas públicas.	12 de septiembre de 2023
Compatibilidad con hibernación para M7i y M7i-flex	Hiberne las instancias recién iniciadas que se ejecutan en tipos de instancia M7i y M7i-flex.	22 de agosto de 2023

EC2-classic ha quedado en desuso.	Con EC2-Classic, las instancias de EC2 se ejecutan en una sola red plana que se comparte con otros clientes. Amazon VPC sustituye a EC2-Classic. Con Amazon VPC, las instancias se ejecutan en una Virtual Private Cloud (VPC) que está aislada lógicamente para su cuenta de AWS.	8 de agosto de 2023
Hosts dedicados	Puede asignar hosts dedicados a activos de hardware específicos de un Outpost.	20 de junio de 2023
Punto de conexión a instancia de EC2	Ahora puede conectarse a una instancia mediante SSH o RDP sin necesidad de que la instancia tenga una dirección IPv4 pública.	13 de junio de 2023
IMDS Package Analyzer	Ahora puede usar el IMDS Package Analyzer para identificar las fuentes de las llamadas de IMDSv1 en sus instancias de EC2.	1 de junio de 2023
Instancias bare metal de la consola serie de EC2	La consola serie de EC2 ahora admite la conectividad con el puerto serie de determinadas instancias bare metal.	11 de abril de 2023

Cuotas de plantilla de inicialización	Ahora puede ver sus cuotas de plantillas de inicialización y versiones de plantillas de inicialización en la consola de Service Quotas y mediante la CLI de Service Quotas.	3 de abril de 2023
Notificaciones de utilización de reservas de capacidad	AWS Healthahora envía notificaciones cuando el uso de la capacidad de reservas de capacidad de su cuenta cae por debajo del 20 por ciento.	3 de abril de 2023
Grupos de reserva de capacidad	Ahora puede agregar reservas de capacidad que se comparten con usted a los grupos de reserva de capacidad que posee.	30 de marzo de 2023
Modificar las opciones de metadatos de instancia	Ahora puede usar la consola Amazon EC2 para modificar las opciones de metadatos de instancia.	20 de marzo de 2023
Actualizaciones locales del sistema operativo macOS	Ahora puede hacer las actualizaciones locales de sistema operativo de macOS de Apple en instancias de M1 de Mac.	14 de marzo de 2023
UEFI preferido	Ahora puede crear una AMI única que admita los modos de arranque Legacy BIOS y Unified Extensible Firmware Interface (UEFI).	3 de marzo de 2023

Modificar una AMI para IMDSv2	Modifique su AMI para que las instancias existentes que se inician desde la AMI requieran IMDSv2 de forma predeterminada.	28 de febrero de 2023
Seguridad basada en la virtualización de Windows: Credential Guard	Puede habilitar Credential Guard, una característica de seguridad basada en la virtualización (VBS), en las instancias de Amazon EC2 compatibles.	31 de enero de 2023
Alias de AMI en plantillas de inicialización	Puede especificar un parámetro AWS Systems Manager en lugar del ID de AMI en las plantillas de inicialización para evitar tener que actualizar las plantillas cada vez que cambie el ID de AMI.	19 de enero de 2023
Compatibilidad con hibernación para C6i, i3en y M6i	Hiberne las instancias recién iniciadas que se ejecutan en tipos de instancias C6i, I3en y M6i.	19 de diciembre de 2022
Prevención de errores de escritura	Mejore el rendimiento de sus cargas de trabajo de base de datos relacional con uso intensivo de E/S y reduzca la latencia sin afectar negativamente a la resiliencia de datos con la prevención de errores de escritura, una característica de almacenamiento en bloques.	29 de noviembre de 2022

ENA Express	Aumente el rendimiento y minimice la latencia final del tráfico de red entre las instancias de EC2 con ENA Express.	28 de noviembre de 2022
Bloqueo de la regla de retención de la papelera de reciclaje	Puede bloquear las reglas de retención para ayudar a protegerlas contra modificaciones y eliminaciones accidentales o malintencionadas.	23 de noviembre de 2022
Copiar etiquetas de AMI	Al copiar una AMI, puede copiar las etiquetas de AMI definidas por el usuario al mismo tiempo.	18 de noviembre de 2022
Tamaño de AMI para almacenar y restaurar	El tamaño de una AMI (antes de la compresión) que se puede almacenar y restaurar en un bucket de Amazon S3 (y desde él) ahora puede ser de hasta 5000 GB.	16 de noviembre de 2022
Estrategia de asignación de priceCapacityOptimized para instancias de spot	Una flota de spot que utilice la estrategia de asignación `priceCapacityOptimized` analiza tanto el precio como la capacidad para seleccionar los grupos de instancias de spot que tienen menos probabilidades de sufrir interrupciones y tienen el precio más bajo posible.	10 de noviembre de 2022

Estrategia de asignación de price-capacity-optimized para instancias de spot	Una flota de EC2 que utilice la estrategia de asignación `price-capacity-optimized` analiza tanto el precio como la capacidad para seleccionar los grupos de instancias de spot que tienen menos probabilidades de sufrir interrupciones y tienen el precio más bajo posible.	10 de noviembre de 2022
Cancelar que se comparta una AMI con su cuenta	Si se ha compartido una AMI con su Cuenta de AWS y ya no desea que sea así, puede eliminar la cuenta de los permisos de inicialización de la AMI.	4 de noviembre de 2022
Transferir direcciones IP elásticas	Ahora puede transferir direcciones IP elásticas de una Cuenta de AWS a otra.	31 de octubre de 2022
Reemplazar un volumen raíz	Puede reemplazar el volumen raíz de Amazon EBS para una instancia en ejecución.	27 de octubre de 2022
Conexión automática de la instancia a la base de datos	Use la característica de conexión automática para conectar rápidamente una o más instancias de EC2 a una base de datos de RDS y permitir el tráfico entre ellas.	10 de octubre de 2022
Cuotas de IAM	Las cuotas ahora se aplican a la creación y al uso compartido de AMI.	10 de octubre de 2022

Configurar AMI para IMDSv2	Configure su AMI para que las instancias que se inician desde la AMI requieran IMDSv2 de forma predeterminada.	3 de octubre de 2022
Iniciar interrupción de instancia de spot	Puede seleccionar una instancia de spot en la consola de Amazon EC2 e iniciar una interrupción para poder probar cómo las aplicaciones de sus instancias de spot gestionan las interrupciones.	26 de septiembre de 2022
Proveedor de AMI verificado	En la consola de Amazon EC2, las AMI públicas que son propiedad de Amazon o de un socio verificado están marcadas con la inscripción Verified provider (Proveedor verificado).	22 de julio de 2022
Grupos de ubicación en AWS Outposts	Se agregó una estrategia de dispersión de host para grupos de ubicación en un Outpost.	30 de junio de 2022
Claves de condición de la papelera de reciclaje	Puede utilizar las claves de condición `rbin:Request/ResourceType` y `rbin:Attribute/ResourceType` para filtrar el acceso en las solicitudes de papelera de reciclaje.	14 de junio de 2022

Volúmenes io2 Block Express	Puede modificar el tamaño y las IOPS aprovisionadas de los volúmenes io2 Block Express y puede habilitarlos para restaurar instantáneas de manera rápida.	31 de mayo de 2022
Hosts dedicados en AWS Outposts	Puede asignar hosts dedicados en AWS Outposts.	31 de mayo de 2022
Protección de detención de instancias	Para evitar que la instancia se detenga de forma accidental, puede habilitar la protección de detención para la instancia.	24 de mayo de 2022
Arranque seguro UEFI	El modo Arranque seguro UEFI se basa en el proceso de arranque seguro consolidado de Amazon EC2 y proporciona protección adicional en profundidad que ayuda a los clientes a proteger el software frente a amenazas que persisten durante los reinicios.	10 de mayo de 2022
NitroTPM	Nitro Trusted Platform Module (NitroTPM, módulo de confianza de la plataforma Nitro) es un dispositivo virtual proporcionado por el sistema Nitro de AWS y cumple con la especificación de TPM 2.0.	10 de mayo de 2022

Eventos de cambio de estado de la AMI	Amazon EC2 ahora genera un evento cuando una AMI cambia de estado. Puede utilizar Amazon EventBridge para detectar y reaccionar a estos eventos.	9 de mayo de 2022
Describa las claves públicas	Puede consultar la clave pública y la fecha de creación de un par de claves de Amazon EC2.	28 de abril de 2022
Creación de pares de claves	Puede especificar el formato de clave (PEM o PPK) al crear un nuevo par de claves.	28 de abril de 2022
Montaje de sistemas de archivos de Amazon FSx en la inicialización	Puede montar un sistema de archivos de Amazon FSx for NetApp ONTAP o Amazon FSx for OpenZFS nuevo o existente durante la inicializ ación con el nuevo asistente de inicialización de instancias.	12 de abril de 2022
Nuevo asistente de inicializ ación de instancias	Una nueva y mejorada experiencia de inicialización en la consola de Amazon EC2 que ofrece una forma más rápida y sencilla de iniciar una instancia de EC2.	5 de abril de 2022
Dé de baja las AMI públicas de forma automática	De forma predeterminada, la fecha de obsolescencia de todas las AMI públicas se establece en dos años a partir de la fecha de creación de la AMI.	31 de marzo de 2022

Categoría de metadatos de instancia: autoscaling/target-lifecycle-state	Cuando se utilizan grupos de Auto Scaling, se puede acceder al estado de ciclo de vida de destino de una instancia desde los metadatos de la instancia.	24 de marzo de 2022
Momento de la última inicialización de la AMI	`lastLaunchedTime` indica cuándo se utilizó la AMI por última vez para iniciar una instancia.	28 de febrero de 2022
Papelera de reciclaje para las AMI	La papelera de reciclaje le permite restaurar las AMI que se eliminaron por accidente.	3 de febrero de 2022
Claves ED25519	Las claves ED25519 ahora son compatibles con instancias de EC2 de Connect y la consola serie de EC2.	20 de enero de 2022
Plataformas RHEL adicionales para reservas de capacidad	Plataformas Red Hat Enterprise Linux adicionales para reservas de capacidad bajo demanda.	11 de enero de 2022
Configurar AMI de Windows para una inicialización más rápido	Configure las AMI de Windows para iniciar instancias hasta un 65 % más rápido y utilice instantáneas aprovisionadas previamente.	10 de enero de 2022
Etiquetas de instancia en los metadatos de instancia	Puede acceder a las etiquetas de una instancia desde los metadatos de la instancia.	6 de enero de 2022

Las reservas de capacidad en grupos con ubicación en clúster	Puede crear reservas de capacidad en grupos de ubicación en clúster.	6 de enero de 2022
Papelera de reciclaje para instantáneas de Amazon EBS	La papelera de reciclaje para instantáneas de Amazon EBS es una característica de recuperación de instantán eas que le permite restaurar instantáneas eliminadas accidentalmente.	29 de noviembre de 2021
Launch-before-terminate de flota de spot	La flota de spot puede terminar las instancias de spot que reciben una notificación de reequilibrio después de iniciar nuevas instancias de spot de reemplazo.	4 de noviembre de 2021
Launch-before-terminate de flota de EC2	La flota de EC2 puede terminar las instancias de spot que reciben una notificación de reequilibrio después de iniciar nuevas instancias de spot de reemplazo.	4 de noviembre de 2021
Comparación de marcas temporales	Puede determinar la hora real de un evento al comparar la marca temporal de la instancia Linux de Amazon EC2 con ClockBound.	2 de noviembre de 2021
Compartir AMI con organizac iones o unidades organizativas	Ahora puede compartir AMI con los siguientes recursos de AWS: organizaciones y unidades organizativas (OU).	29 de octubre de 2021

Puntuación de ubicación de spot	Reciba una recomendación para una región o zona de disponibilidad de AWS según sus requisitos de capacidad de spot.	27 de octubre de 2021
Selección de tipo de instancia basada en atributos para la flota de spot	Especifique los atributos que debe tener una instancia y Amazon EC2 identificará todos los tipos de instancias con esos atributos.	27 de octubre de 2021
Selección de tipo de instancia basada en atributos para la flota de EC2	Especifique los atributos que debe tener una instancia y Amazon EC2 identificará todos los tipos de instancias con esos atributos.	27 de octubre de 2021
Flota de Reservas de capacidad en diferido	Puede utilizar una Flota de Reservas de capacidad para iniciar un grupo, o flota, de Reservas de capacidad.	5 de octubre de 2021
Soporte de hibernación para Ubuntu 20.04 LTS - Focal	Hiberne las instancias recién iniciadas que se iniciaron desde la AMI de Ubuntu 20.04 LTS - Focal.	4 de octubre de 2021
Flota de EC2 y reservas de capacidad bajo demanda seleccionadas	La flota de EC2 puede iniciar instancias bajo demanda en las reservas de capacidad de `targeted`.	22 de septiembre de 2021
Instancias T3 en hosts dedicados	Soporte para instancias T3 en un host dedicado de Amazon EC2.	14 de septiembre de 2021

Compatibilidad de hibernación para RHEL, Fedora y CentOS	Hiberne las instancias recién iniciadas de las AMI de RHEL, Fedora y CentOS.	9 de septiembre de 2021
Amazon EC2 Global View	Amazon EC2 Global View permite ver VPC, subredes, instancias, grupos de seguridad y volúmenes en varias regiones de AWS en una sola consola.	1 de septiembre de 2021
Compatibilidad con la obsolescencia de AMI para Amazon Data Lifecycle Manager	Las políticas de AMI respaldadas por EBS de Amazon Data Lifecycle Manager pueden dar de baja las AMI. La política administrada de AWS AWSDataLifecycleManagerServiceRoleForAMIManagement se ha actualizado para admitir esta característica.	23 de agosto de 2021
Compatible con la hibernación para C5d, M5d y R5d	Hiberne las instancias recién iniciadas que se ejecutan en tipos de instancias C5d, M5d y R5d.	19 de agosto de 2021
Pares de claves de Amazon EC2	Amazon EC2 ahora admite claves ED25519 en instancias de Linux y Mac.	17 de agosto de 2021
Prefijos de las interfaces de red	Puede asignar un intervalo CIDR IPv4 o IPv6 privado, ya sea de forma automática o manual, a las interfaces de red.	22 de julio de 2021

Periodos de eventos	Puede definir periodos de eventos semanales personalizados para eventos programados que reinicien , detengan o terminen sus instancias de Amazon EC2.	15 de julio de 2021
Compatibilidad con el etiquetado y los ID de recursos para las reglas de los grupos de seguridad	Puede consultar las reglas de los grupos de seguridad mediante el ID del recurso. También puede agregar etiquetas a las reglas de los grupos de seguridad.	7 de julio de 2021
Dar de baja una AMI	Ahora puede especificar cuándo una AMI se vuelve obsoleta.	11 de junio de 2021
Facturación por segundo de Windows	Amazon EC2 cobra el uso basado en Windows y SQL Server por segundos, con un cargo mínimo de un minuto.	10 de junio de 2021
Reservas de capacidad en AWS Outposts	Ahora puede utilizar reservas de capacidad en AWS Outposts.	24 de mayo de 2021
Uso compartido de reserva de capacidad	Ahora se puede compartir las Reservas de capacidad y usarlas en Local Zones y zonas Wavelength.	24 de mayo de 2021
Reemplazo del volumen raíz	Ahora puede utilizar tareas de reemplazo de volumen raíz con el fin de reemplazar el volumen de EBS raíz para instancias en ejecución.	22 de abril de 2021

Almacenar y restaurar una AMI mediante S3	Almacene AMI respaldadas por EBS en S3 y restáurelas desde S3 para permitir la copia de AMI entre particiones.	6 de abril de 2021
Consola serie de EC2	Solucione problemas de arranque y conectividad de red estableciendo una conexión con el puerto de serie de una instancia.	30 de marzo de 2021
Modos de arranque	Amazon EC2 ahora es compatible con el arranque UEFI en instancias de EC2 basadas en AMD e Intel seleccionadas.	22 de marzo de 2021
Crear un registro de DNS inverso	Ahora puede configurar la búsqueda DNS inversa para las direcciones IP elásticas.	3 de febrero de 2021
Etiquetar las AMI y las instantáneas en la creación de la AMI	Cuando crea una AMI, puede asignar etiquetas a la AMI y las instantáneas con las mismas etiquetas o puede asignarles etiquetas diferentes.	4 de diciembre de 2020
Uso de Amazon EventBridge para monitorear eventos de flota de spot	Cree reglas de EventBridge que desencadenen acciones programáticas en respuesta a cambios de estado y errores de la flota de spot.	20 de noviembre de 2020

Uso de Amazon EventBridge para monitorear eventos de flota de EC2	Cree reglas de EventBridge que activen acciones programáticas en respuesta a cambios de estado flota de EC2 y errores.	20 de noviembre de 2020
Eliminar flotas instant	Elimine un flota de EC2 de tipo `instant` y termine todas las instancias de la flota en una sola llamada de API.	18 de noviembre de 2020
Compatibilidad de la hibernación con T3 y T3a	Hiberne las instancias recién iniciadas que se ejecutan en tipos de instancias T3 y T3a.	17 de noviembre de 2020
Amazon EFS Quick Create	Puede crear y montar un sistema de archivos de Amazon EFS en una instancia al lanzarla mediante Amazon EFS Quick Create.	9 de noviembre de 2020
Categorías de metadatos de instancia: events/recommendations/rebalance	Tiempo aproximado, en UTC, en el que se emite la notificación de recomendación de reequilibrio de la instancia de EC2 para la instancia.	4 de noviembre de 2020
Recomendación de reequilibrio de instancia de EC2	Una señal que lo notifica cuando una instancia de spot está en riesgo elevado de interrupción.	4 de noviembre de 2020
Reservas de capacidad en zonas Wavelength	Ahora se puede crear el Reservas de capacidad y usarlo en zonas Wavelength.	4 de noviembre de 2020

Reequilibrio de la capacidad	Configure la flota de spot o la flota de EC2 para iniciar una instancia de spot de reemplazo cuando Amazon EC2 emita una recomendación de reequilibrio.	4 de noviembre de 2020
Compatibilidad de la hibernación con I3, M5ad y R5ad	Hiberne las instancias recién iniciadas que se ejecutan en tipos de instancia I3, M5ad y R5ad.	21 de octubre de 2020
Límites de vCPU de instancias de spot	Los límites de instancias de spot ahora se administran en términos de la cantidad de vCPU que usan o usarán sus instancias de spot en ejecución hasta que se satisfaga el límite de solicitud es abiertas.	1 de octubre de 2020
Reservas de capacidad en zonas locales	Ahora se pueden crear y usar Reservas de capacidad en Local Zones.	30 de septiembre de 2020
Compatibilidad de la hibernación con M5a y R5a	Hiberne las instancias recién iniciadas que se ejecutan en tipos de instancias M5a y R5a.	28 de agosto de 2020
Los metadatos de la instancia proporcionan información sobre el lugar y la ubicación de la instancia	Nuevos campos de metadatos de instancia en la categoría `placement` : Región, nombre del grupo de ubicación, número de partición, ID de host e ID de zona de disponibilidad.	24 de agosto de 2020

Grupos de reserva de capacidad	Puede utilizar AWS Resource Groups para crear coleccion es lógicas de reservas de capacidad y, a continuación, iniciar instancias de destino en esos grupos.	29 de julio de 2020
EC2Launch v2	Puede utilizar EC2Launch v2 para realizar tareas durante el inicio de la instancia, si se detiene una instancia y se inicia posteriormente, si se reinicia una instancia y bajo demanda. EC2Launch v2 admite todas las versiones de Windows Server y reemplaza EC2Launch y EC2Config.	30 de junio de 2020
Traer sus propias direcciones IPv6	Puede traer parte o todo su intervalo de direcciones IPv6 de su red en las instalaciones a su cuenta de AWS.	21 de mayo de 2020
Iniciar instancias con un parámetro de Systems Manager	Puede especificar un parámetro AWS Systems Manager en lugar de una AMI al iniciar una instancia.	5 de mayo de 2020
Personalizar notificaciones de eventos programados	Puede personalizar las notificaciones de eventos programados para incluir etiquetas en la notificación de correo electrónico.	4 de mayo de 2020

Kernel Live Patching de Amazon Linux 2	Kernel Live Patching para Amazon Linux 2 permite aplicar parches de vulnerabilidad de seguridad y errores críticos a un kernel de Linux en ejecución, sin reinicios ni interrupciones en las aplicaciones en ejecución.	28 de abril de 2020
Windows Server en hosts dedicados	Puede utilizar las AMI de Windows Server proporcionadas por Amazon para ejecutar las versiones más recientes de Windows Server en hosts dedicados.	7 de abril de 2020
Detener e iniciar una instancia de spot	Detenga las instancias de spot respaldadas por Amazon EBS y vuelva a iniciarlas a voluntad, en lugar de confiar en el comportamiento de interrupción de parada.	13 de enero de 2020

Etiquetado de recursos	Puede etiquetar puertas de enlace de Internet de solo salida, puertas de enlace locales, tablas de enrutamiento de puertas de enlace locales, interfaces virtuales de puertas de enlace local, grupos de interfaces virtuales de puertas de enlace locales, asociaciones de VPC de tablas de enrutamiento de puertas de enlace locales y asociaciones de grupos de interfaz virtual de tablas de enrutamiento de puertas de enlace locales.	10 de enero de 2020
Conectarse a su instancia con Session Manager	Puede iniciar una sesión del Administrador de sesiones con una instancia desde la consola de Amazon EC2.	18 de diciembre de 2019
Host dedicados y grupos de recursos de host	Los hosts dedicados se pueden utilizar ahora con grupos de recursos de host.	2 de diciembre de 2019
Uso compartido de host dedicado	Ahora puede compartir sus hosts dedicados en las cuentas de AWS.	2 de diciembre de 2019
Especificación de crédito predeterminada en el nivel de cuenta	Puede establecer la especificación de crédito predeterminada por familia de instancias de rendimiento ampliable en el nivel de cuenta por región de AWS.	25 de noviembre de 2019

Detección de tipos de instancia	Puede encontrar un tipo de instancia que satisfaga sus necesidades.	22 de noviembre de 2019
Hosts dedicados	Ahora puede configurar un host dedicado para que admita varios tipos de instancia en una familia de instancias.	21 de noviembre de 2019
Servicio de metadatos de instancia, versión 2	Puede usar Servicio de metadatos de instancia versión 2, que es un método orientado a la sesión para solicitar metadatos de instancia.	19 de noviembre de 2019
Elastic Fabric Adapter	Ahora los Elastic Fabric Adapter se pueden usar con Intel MPI 2019 actualización 6.	15 de noviembre de 2019
Compatibilidad de la hibernación con instancias bajo demanda de Windows	Puede hibernar las instancias bajo demanda de Windows.	14 de octubre de 2019
Compras en cola de instancias reservadas	Puede poner en cola una compra de una instancia reservada hasta tres años por adelantado.	4 de octubre de 2019
Interrupción de diagnóstico	Puede enviar una interrupción de diagnóstico a una instancia inaccesible o que no responde para activar un pánico de kernel.	14 de agosto de 2019

Estrategia de asignación optimizada de la capacidad	Mediante la flota de EC2 o la flota de spot, puede iniciar instancias de spot desde grupos de spot con una capacidad óptima para la cantidad de instancias que se van a iniciar.	12 de agosto de 2019
Uso compartido de reserva de capacidad bajo demanda	Ahora puede compartir sus reservas de capacidad en las cuentas de AWS.	29 de julio de 2019
Elastic Fabric Adapter	EFA ahora admite Open MPI 3.1.4 e Intel MPI 2019 Update 4.	26 de julio de 2019
Conexión de instancia de EC2	EC2 Instance Connect es una forma simple y segura de conectarse a sus instancias utilizando Secure Shell (SSH).	27 de junio de 2019
Recuperación de host	Reinicia automáticamente sus instancias en un nuevo host en caso de un fallo de hardware inesperada en un host dedicado.	5 de junio de 2019
Instantáneas coherentes con la aplicación de VSS	Tome instantáneas coherentes con la aplicación de todos los volúmenes de Amazon EBS adjuntados a sus instancia s de Windows mediante AWS Systems Manager Run Command.	13 de mayo de 2019

Asistente de cambio de plataforma de Windows a Linux para las bases de datos de Microsoft SQL Server	Transfiera cargas de trabajo de Microsoft SQL Server de un sistema operativo Windows a uno Linux.	8 de mayo de 2019
Actualización automatizada de Windows	Realice actualizaciones automatizadas de instancias de Windows de EC2 mediante AWS Systems Manager.	6 de mayo de 2019
Elastic Fabric Adapter	Puede adjuntar un Elastic Fabric Adapter a sus instancias para acelerar las aplicaciones de informática de alto rendimiento (HPC).	29 de abril de 2019

Para obtener información sobre las versiones de tipos de instancias para Amazon EC2, consulte Historial de documentos en la Guía de tipos de instancias de Amazon EC2.

Historial de 2018 y anteriores

En la siguiente tabla se describen los cambios importantes de la Guía del usuario de Amazon EC2 de 2018 y años anteriores.

Característica	Versión de API	Descripción	Fecha de la versión
Grupos de ubicación de particiones	15/11/2016	Los grupos de ubicación de particiones reparten las instancias entre particiones lógicas y garantizan que las instancias de una partición no compartan el hardware subyacente con las de otras particiones. Para obtener más información, consulte Grupos de ubicación de particiones.	20 de diciembre de 2018

Característica	Versión de API	Descripción	Fecha de la versión
Hibernar instancias de EC2 de Linux	15/11/2016	Puede hibernar una instancia Linux si está habilitada para la hibernación y cumple con los requisitos previos de hibernación. Para obtener más información, consulte Hibernación de la instancia de Amazon EC2.	28 de noviembre de 2018
Aceleradores de Amazon Elastic Inference	15/11/2016	Puede asociar un acelerador de Amazon EI a sus instancias para añadir aceleración basadas en GPU para reducir el costo de ejecución de inferencia de aprendizaje profundo.	28 de noviembre de 2018
La consola de spot recomienda una flota de instancias	15/11/2016	La consola de spot recomienda una flota de instancias basadas en las prácticas recomendadas de spot (diversificación de instancias) para cumplir con las especificaciones de hardware mínimas (CPU virtuales, memoria y almacenamiento) que necesita para su aplicación. Para obtener más información, consulte Creación de una solicitud de flota de spot.	20 de noviembre de 2018
Nuevo tipo de solicitud de flota de EC2: instant	15/11/2016	La flota de EC2 es ahora compatible con un nuevo tipo de solicitud, `instant`, que puede utilizar para aprovisionar de forma sincrónica la capacidad en los tipos de instancia y modelos de compra. La solicitud `instant` devuelve las instancias iniciadas en la respuesta de la API y no realiza ninguna acción más, lo que le permite controlar si se inician instancias o cuándo se inician. Para obtener más información, consulte Tipos de solicitudes de flota de EC2.	14 de noviembre de 2018

Característica	Versión de API	Descripción	Fecha de la versión
Información de ahorro de spot	15/11/2016	Puede ver los ahorros obtenidos mediante el uso de instancias de spot para una sola flota de spot o para todas las instancias de spot. Para obtener más información, consulte Ahorro en la compra de instancias de spot.	5 de noviembre de 2018
Compatibilidad de la consola para la optimización de opciones de la CPU	15/11/2016	Al iniciar una instancia, puede optimizar las opciones de CPU para que se adapten a cargas de trabajo o necesidades empresariales mediante la consola de Amazon EC2. Para obtener más información, consulte Optimización de las opciones de CPU.	31 de octubre de 2018
Compatibilidad de la consola para la creación de una plantilla de inicialización desde una instancia	15/11/2016	Puede crear una plantilla de inicialización mediante una instancia como base para una nueva plantilla de inicialización mediante la consola de Amazon EC2. Para obtener más información, consulte Creación de una plantilla de lanzamiento.	30 de octubre de 2018
On-Demand Capacity Reservations	15/11/2016	Puede reservar capacidad para sus instancias de Amazon EC2 en una zona de disponibilidad específica para cualquier duración. Esto le permite crear y administrar reservas de capacidad de forma independiente de los descuentos de facturación ofrecidos por instancias reservadas. Para obtener más información, consulte On-Demand Capacity Reservations.	25 de octubre de 2018

Característica	Versión de API	Descripción	Fecha de la versión
Traiga sus propias direcciones IP (del inglés BYOIP)	15/11/2016	Puede traer parte o todo su intervalo de direcciones IPv4 públicas de su red en las instalaciones a su cuenta de AWS. Una vez que traiga su gama de direcciones a AWS, aparecerá en su cuenta como un grupo de direcciones. Puede crear una dirección IP elástica a partir de su grupo de direcciones y utilizarla con los recursos de AWS. Para obtener más información, consulte Traiga sus propias direcciones IP (BYOIP) en Amazon EC2.	23 de octubre de 2018
Etiqueta de host dedicado en el momento de la creación y compatibilidad de la consola	15/11/2016	Puede etiquetar hosts dedicados en el momento de su creación y puede administrar las etiquetas de host dedicado mediante la consola de Amazon EC2. Para obtener más información, consulte Asignar hosts dedicados.	08 de octubre de 2018
Compatibilidad de la consola con el escalado programado para la flota de spot	15/11/2016	Permite aumentar o reducir la capacidad actual de la flota en función de la fecha y la hora. Para obtener más información, consulte Escalado de la flota de spot mediante el escalado programado.	20 de septiembre de 2018
Estrategias de asignación de Flotas de EC2	15/11/2016	Puede especificar si la capacidad bajo demanda se cubrirá en función del precio (primero las de precio más bajo) o de la prioridad (primero las de mayor prioridad). Puede especificar el número de grupos de spot en los que asignar la capacidad de spot de destino. Para obtener más información, consulte Estrategias de asignación de instancias de spot.	26 de julio de 2018

Característica	Versión de API	Descripción	Fecha de la versión
Estrategias de asignación de Flotas de spot	15/11/2016	Puede especificar si la capacidad bajo demanda se cubrirá en función del precio (primero las de precio más bajo) o de la prioridad (primero las de mayor prioridad). Puede especificar el número de grupos de spot en los que asignar la capacidad de spot de destino. Para obtener más información, consulte Estrategias de asignación de instancias de spot.	26 de julio de 2018
Automatización del ciclo de vida de instantáneas	15/11/2016	Puede usar Amazon Data Lifecycle Manager para automatizar la creación y eliminación de instantáneas de los volúmenes de EBS. Para obtener más información, consulte Amazon Data Lifecycle Manager.	12 de julio de 2018
Opciones de CPU de la plantilla de inicialización	15/11/2016	Cuando crea una plantilla de inicialización mediante las herramientas de la línea de comandos, puede optimizar las opciones de CPU para que se adapten a cargas de trabajo o necesidades del negocio específicas. Para obtener más información, consulte Creación de una plantilla de lanzamiento.	11 de julio de 2018
Etiquetar hosts dedicados	15/11/2016	Puede etiquetar sus hosts dedicados. Para obtener más información, consulte Etiquetar hosts dedicados.	3 de julio de 2018
Obtención de la salida más reciente de la consola	15/11/2016	Puede recuperar la salida más reciente de la consola para algunos tipos de instancias si utiliza el comando get-console-output de la AWS CLI.	9 de mayo de 2018

Característica	Versión de API	Descripción	Fecha de la versión
Optimización de las opciones de CPU	15/11/2016	Al iniciar una instancia, puede optimizar las opciones de CPU para que se adapten a cargas de trabajo o necesidades empresariales específicas. Para obtener más información, consulte Optimización de las opciones de CPU.	8 de mayo de 2018
EC2 Fleet	15/11/2016	Puede utilizar la flota de EC2 para iniciar un grupo de instancias en diferentes tipos de instancias de EC2 y zonas de disponibilidad, así como en modelos de compra de instancia bajo demanda, instancia reservada e instancia de spot. Para obtener más información, consulte Flota de EC2.	2 de mayo de 2018
Instancias bajo demanda en flotas de spot	15/11/2016	Puede incluir una solicitud de capacidad bajo demanda en su solicitud de flota de spot para asegurarse de que siempre dispone de capacidad de instancia. Para obtener más información, consulte Flota de spot.	2 de mayo de 2018
Etiquetado de instantáneas de EBS durante la creación	15/11/2016	Puede aplicar etiquetas a las instantáneas en el momento de su creación.	2 de abril de 2018
Cambio de los grupos de ubicación	15/11/2016	Puede mover una instancia dentro o fuera de un grupo de ubicación, o cambiar su grupo de ubicación. Para obtener más información, consulte Cambiar el grupo de ubicación para una instancia.	1 de marzo de 2018
ID de recursos más largos	15/11/2016	Puede habilitar el formato de ID de más longitud para más tipos de recursos. Para obtener más información, consulte ID de recursos.	9 de febrero de 2018

Característica	Versión de API	Descripción	Fecha de la versión
Mejoras en el rendimiento de red	15/11/2016	Las instancias fuera de un grupo con ubicación en clúster pueden beneficiarse ahora del mayor ancho de banda al enviar o recibir tráfico de red entre otras instancias o Amazon S3.	24 de enero de 2018
Etiquetar direcciones IP elásticas	15/11/2016	Puede etiquetar sus direcciones IP elásticas . Para obtener más información, consulte Etiquetado de una dirección IP elástica.	21 de diciembre de 2017
Servicio de sincronización temporal de Amazon	15/11/2016	Puede usar el Servicio de sincronización temporal de Amazon para mantener la hora correcta en su instancia. Para obtener más información, consulte Establezca el tiempo de su instancia de Amazon EC2..	29 de noviembre de 2017
T2 Unlimited	15/11/2016	Las instancias T2 Unlimited pueden realizar ráfagas por encima de la base de referencia durante el tiempo que sea necesario. Para obtener más información, consulte Instancias de rendimiento ampliable.	29 de noviembre de 2017
Plantillas de inicialización	15/11/2016	Una plantilla de inicialización puede contener algunos o todos los parámetros para iniciar una instancia, de modo que no tenga que especificarlos cada vez que vaya a iniciar una. Para obtener más información, consulte iniciar una instancia desde una plantilla de inicialización.	29 de noviembre de 2017
Ubicación distribuida	15/11/2016	Se recomienda usar grupos de ubicación distribuida en aplicaciones con pocas instancias críticas que deben mantenerse separadas entre sí. Para obtener más información, consulte Grupos de ubicación distribuida.	29 de noviembre de 2017

Característica	Versión de API	Descripción	Fecha de la versión
Hibernación de instancias de spot	15/11/2016	El servicio de spot puede hibernar instancias de spot en caso de una interrupción. Para obtener más información, consulte Hibernar instancias de spot interrumpida.	28 de noviembre de 2017
Seguimiento de destino de flota de spot	15/11/2016	Puede configurar políticas de escalado de seguimiento de destino de su flota de spot. Para obtener más información, consulte Escalado de una flota de spot con una política de seguimiento de destino.	17 de noviembre de 2017
La flota de spot se integra con Elastic Load Balancing	15/11/2016	Puede adjuntar uno o más equilibradores de carga a una flota de spot.	10 de noviembre de 2017
Fusión y división de instancias reservadas convertibles	15/11/2016	Puede intercambiar (fusionar) dos o más instancias reservadas convertibles para obtener una instancia reservada convertible nueva. También puede usar el proceso de modificación para dividir una instancia reservada convertible en reservas más pequeñas. Para obtener más información, consulte Intercambiar instancias reservadas convertibles.	6 de noviembre de 2017
Modificación de la tenencia de VPC	15/11/2016	Puede cambiar el atributo de tenencia de instancia de una VPC de `dedicated` a `default`. Para obtener más información, consulte Cambiar la propiedad de una VPC.	16 de octubre de 2017
Facturación por segundo	15/11/2016	Amazon EC2 cobra el uso basado en Linux por segundos, con un cargo mínimo de un minuto.	2 de octubre de 2017

Característica	Versión de API	Descripción	Fecha de la versión
Detención en caso de interrupción	15/11/2016	Puede especificar si Amazon EC2 debe hibernar, detener o terminar las instancias de spot cuando se interrumpen. Para obtener más información, consulte Comportamiento de las interrupciones de las instancias de spot.	18 de septiembre de 2017
Etiquetado de puertas de enlace NAT	15/11/2016	Puede etiquetar su puerta de enlace NAT. Para obtener más información, consulte Etiquetar los recursos.	7 de septiembre de 2017
Descripciones de regla de grupo de seguridad	15/11/2016	Puede agregar descripciones a sus reglas de grupo de seguridad. Para obtener más información, consulte Reglas del grupo de seguridad.	31 de agosto de 2017
Elastic Graphics	15/11/2016	Asocie aceleradores de Elastic Graphics a las instancias para acelerar el rendimiento de los gráficos de las aplicaciones.	29 de agosto de 2017
Recuperar las direcciones IP elásticas	15/11/2016	Si libera una dirección IP elástica para su uso en una VPC, es posible que pueda recuperar la. Para obtener más información, consulte Recuperar una dirección IP elástica.	11 de agosto de 2017
Etiquetar instancias de flota de spot	15/11/2016	Puede configurar su flota de spot de modo que se etiqueten de forma automática las instancias que lance.	24 de julio de 2017

Característica	Versión de API	Descripción	Fecha de la versión
Recursos de etiquetas durante la creación	15/11/2016	Puede aplicar etiquetas a instancias y volúmenes en el momento de su creación. Para obtener más información, consulte Etiquetar los recursos. Asimismo, puede utilizar permisos de nivel de recurso basados en etiquetas para controlar las etiquetas que se aplican. Para obtener más información, consulte Conceder permisos para etiquetar recursos durante la creación.	28 de marzo de 2017
Realizar modificaciones en volúmenes de EBS conectados	15/11/2016	Con la mayoría de los volúmenes de EBS adjuntos a la mayoría de las instancias de EC2, puede modificar el tamaño, el tipo y el IOPS del volumen sin separarlo ni detener la instancia.	13 de febrero de 2017
Asociar un rol de IAM	15/11/2016	Puede adjuntar, separar o reemplazar un rol de IAM de una instancia existente. Para obtener más información, consulte Roles de IAM para Amazon EC2.	9 de febrero de 2017
Instancias de spot dedicado.	15/11/2016	Puede ejecutar instancias de spot en hardware de un solo propietario en una nube privada virtual (VPC). Para obtener más información, consulte Especificar una tenencia para su instancias de spot.	19 de enero de 2017
Compatibilidad con IPv6	15/11/2016	Puede asociar un bloque de CIDR IPv6 a la VPC y subredes y asignar direcciones IPv6 a las instancias de la VPC. Para obtener más información, consulte Direccionamiento IP de instancias Amazon EC2.	1 de diciembre de 2016

Característica	Versión de API	Descripción	Fecha de la versión
Escalado automático para la flota de spot		Ahora puede configurar políticas de escalado para su flota de spot. Para obtener más información, consulte Escalado automático para la flota de spot.	1 de septiembre de 2016
Elastic Network Adapter (ENA)	01/04/2016	Ahora puede utilizar ENA para disfrutar de redes mejoradas. Para obtener más información, consulte Se ha mejorado la compatibilidad de red.	28 de junio de 2016
Soporte mejorado para ver y modificar ID más largos	01/04/2016	Ahora puede ver y modificar configuraciones de ID más largas para otros usuarios de IAM, roles de IAM o para el usuario raíz. Para obtener más información, consulte ID de recursos.	23 de junio de 2016
Copie las instantáneas de Amazon EBS cifradas entre cuentas de AWS	01/04/2016	Ahora puede copiar instantáneas de EBS cifradas entre cuentas de AWS.	21 de junio de 2016
Captura de pantalla de una consola de instancias	01/10/2015	Ahora puede obtener información adicional cuando depure instancias que son inaccesibles. Para obtener más información, consulte Captura de pantalla de una instancia inaccesible.	24 de mayo de 2016
Dos nuevos tipos de volúmenes de EBS	01/10/2015	Ahora puede crear volúmenes de HDD de rendimiento optimizado (st1) y HDD en frío (sc1).	19 de abril de 2016
Se han añadido nuevas métricas NetworkPacketsIn y NetworkPacketsOut para Amazon EC2		Se han añadido nuevas métricas NetworkPacketsIn y NetworkPacketsOut para Amazon EC2. Para obtener más información, consulte Métricas de la instancia.	23 de marzo de 2016

Característica	Versión de API	Descripción	Fecha de la versión
Métricas de CloudWatch para las flotas de spot		Ahora puede obtener métricas de CloudWatch para su flota de spot. Para obtener más información, consulte Métricas de CloudWatch para las flotas de spot.	21 de marzo de 2016
Instancias programadas	01/10/2015	Con las instancias reservadas programadas (instancias programadas), puede adquirir reservas de capacidad que se repiten a diario, semanal o mensualmente con una hora de inicio y duración específicos.	13 de enero de 2016
ID de recursos más largos	01/10/2015	Estamos introduciendo gradualmente ID de mayor longitud para algunos tipos de recursos de Amazon EC2 y Amazon EBS. Durante el período de inscripción, podrá habilitar el formato de ID de más longitud para los tipos de recursos admitidos. Para obtener más información, consulte ID de recursos.	13 de enero de 2016
Soporte de DNS ClassicLink	01/10/2015	Puede habilitar la compatibilidad de DNS con ClassicLink en la VPC para que los nombres de host DNS que se direccionan entre las instancias de EC2-Classic vinculadas y las instancias de la VPC se resuelvan en direcciones IP privadas y no en direcciones IP públicas.	11 de enero de 2016
Hosts dedicados	01/10/2015	Un host dedicado de Amazon EC2 es un servidor físico con capacidad de instancias dedicado a su uso. Para obtener más información, consulte Dedicated Hosts.	23 de noviembre de 2015
Duración de instancias de spot	01/10/2015	Ahora puede especificar la duración de sus instancias de spot. No se admiten bloques de spot (enero de 2023).	6 de octubre de 2015

Característica	Versión de API	Descripción	Fecha de la versión
Solicitud de modificación de la flota de spot	01/10/2015	Ahora puede modificar la capacidad de destino de su solicitud de la flota de spot. Para obtener más información, consulte Modificación de una solicitud de flota de spot.	29 de septiembre de 2015
Estrategia de asignación diversificada de la flota de spot	15/04/2015	Ahora puede asignar instancias de spot en varios grupos de spot mediante una sola solicitud de flota de spot. Para obtener más información, consulte Estrategias de asignación de instancias de spot.	15 de septiembre de 2015
Ponderación de instancias de flota de spot	15/04/2015	Ahora puede definir las unidades de capacidad con la que contribuye cada tipo de instancia al rendimiento de la aplicación y ajustar el precio de puja de instancias de spot de cada grupo de spot de la manera correspondiente. Para obtener más información, consulte Ponderación de instancias de flota de spot.	31 de agosto de 2015
Nueva acción de alarma de reinicio y nuevo rol de IAM para su uso con acciones de alarma		Se ha añadido la acción de alarma de reinicio y nuevo rol de IAM para su uso con acciones de alarma. Para obtener más información, consulte Crear alarmas que detienen, terminan, reinician o recuperan una instancia.	23 de julio de 2015
Spot Fleets	15/04/2015	Puede administrar una colección o flota de instancias de spot en lugar de administrar diferentes solicitudes de instancias de spot. Para obtener más información, consulte Flota de spot.	18 de mayo de 2015
Migración de direcciones IP elásticas a EC2-Classic	15/04/2015	Puede migrar una dirección IP elástica que asignó para usarla en EC2-Classic para que se utilice en una VPC.	15 de mayo de 2015

Característica	Versión de API	Descripción	Fecha de la versión
Importación de máquinas virtuales con varios discos como AMI	01/03/2015	El proceso de VM Import ahora también admite la importación de máquinas virtuales con varios discos como AMI. Para obtener más información, consulte Importación de una VM como una imagen utilizando VM Import/Export en la Guía del usuario de VM Import/Export.	23 de abril de 2015
Systems Manager		Systems Manager le permite configurar y administrar sus instancias de EC2.	17 de febrero de 2015
Systems Manager para Microsoft SCVMM 1.5		Ahora puede utilizar Systems Manager para Microsoft SCVMM para iniciar una instancia e importar una máquina virtual de SCVMM a Amazon EC2.	21 de enero de 2015
Recuperación automática para instancias de EC2		Puede crear una alarma de Amazon CloudWatch que supervise una instancia de Amazon EC2 y recupere de forma automática la instancia si deja de funcionar debido a un error de hardware subyacente o un problema que requiera la intervención de AWS en la reparación. Una instancia recuperada es idéntica a la instancia original, incluido el ID de instancia, las direcciones IP y todos los metadatos de la instancia. Para obtener más información, consulte Resiliencia de las instancias.	12 de enero de 2015

Característica	Versión de API	Descripción	Fecha de la versión
ClassicLink	01/10/2014	Con ClassicLink, puede enlazar una instancia de EC2-Classic a una VPC de su cuenta. Puede asociar los grupos de seguridad de VPC a la instancia de EC2-Classic, lo que hace posible la comunicación entre la instancia de EC2-Classic y las instancias de la VPC utilizando direcciones IP privadas.	7 de enero de 2015
Avisos de terminación de instancias de spot		La mejor forma de protegerse frente a una interrupción de una instancia de spot es diseñar su aplicación con tolerancia a errores. Asimismo, puede beneficiarse de los avisos de terminación de una instancia de spot, que envían una advertencia dos minutos antes de que Amazon EC2 tenga que detener o terminar su instancia de spot. Para obtener más información, consulte Avisos de interrupción de instancias de spot..	5 de enero de 2015
Systems Manager Microsoft SCVMM		Systems Manager para Microsoft SCVMM proporciona una interfaz sencilla y fácil de usar para la administración de los recursos de AWS, por ejemplo, las instancias de EC2, desde Microsoft SCVMM.	29 de octubre de 2014
Soporte de paginación de `DescribeVolumes`	01/09/2014	Ahora, la llamada a la API `DescribeVolumes` permite la paginación de resultados con los parámetros `MaxResults` y `NextToken`. Para obtener más información, consulte DescribeVolumes en la Amazon EC2 API Reference.	23 de octubre de 2014

Característica	Versión de API	Descripción	Fecha de la versión
Se ha agregado compatibilidad para Amazon CloudWatch Logs		Puede utilizar registros de Amazon CloudWatch para monitorizar, almacenar y obtener acceso a los archivos de registro del sistema, aplicación y personalizados desde instancias u otras fuentes. A continuación, puede recuperar los datos de registro asociados desde CloudWatch Logs mediante la consola de Amazon CloudWatch, los comandos de CloudWatch Logs en la AWS CLI o el SDK de CloudWatch Logs.	10 de julio de 2014
Nueva página EC2 Service Limits (Límites de los servicios de EC2)		Utilice la página EC2 Service Limits (Límites de los servicios de EC2) de la consola de Amazon EC2 para ver los límites actuales de los recursos que proporcionan Amazon EC2 y Amazon VPC, por cada región.	19 de junio de 2014
Volúmenes SSD de uso general de Amazon EBS	01/05/2014	Los volúmenes SSD de uso general ofrecen almacenamiento económico que resulta ideal para una gran variedad de cargas de trabajo. Estos volúmenes ofrecen latencias en milisegundos de un solo dígito, la posibilidad de ampliar a 3000 IOPS durante periodos prolongados y un rendimiento de referencia de 3 IOPS/GiB. El tamaño de un volumen SSD de uso general puede variar de 1 GiB a 1 TiB.	16 de junio de 2014
AWS Management Pack		AWS Management Pack ahora admite System Center Operations Manager 2012 R2.	22 de mayo de 2014

Característica	Versión de API	Descripción	Fecha de la versión
Amazon EBS encryption	01/05/2014	Cifrado de Amazon EBS ofrece un cifrado perfecto de volúmenes de datos de EBS e instantáneas, lo que elimina la necesidad de crear y mantener una infraestructura de administración de claves segura. El cifrado de EBS permite la seguridad de los datos en reposo mediante el cifrado de los datos con Claves administradas por AWS. El cifrado se produce en los servidores que alojan las instancias de EC2, por lo que los datos se cifran a medida que circulan entre las instancias de EC2 y el almacenamiento de EBS.	21 de mayo de 2014
Informes de uso de Amazon EC2		Los informes de uso de Amazon EC2 son un conjunto de informes que muestran datos de costo y uso sobre su uso de EC2.	28 de enero de 2014
Importación de máquinas virtuales Linux	15/10/2013	El proceso de VM Import ahora también admite la importación de instancias Linux. Para obtener más información, consulte la Guía del usuario de VM Import/Export.	16 de diciembre de 2013
Permisos de nivel de recursos para RunInstances	15/10/2013	Ahora puede crear políticas en AWS Identity and Access Management para controlar los permisos de nivel de recursos para la acción de la API RunInstances de Amazon EC2. Para obtener más información y políticas de ejemplo, consulte Identity and Access Management para Amazon EC2.	20 de noviembre de 2013

Característica	Versión de API	Descripción	Fecha de la versión
Inicialización de una instancia desde AWS Marketplace		Ahora puede iniciar una instancia desde AWS Marketplace con el asistente de inicialización de Amazon EC2. Para obtener más informaci ón, consulte iniciar una AWS Marketplace instancia.	11 de noviembre de 2013
Nuevo launch wizard		Se ha rediseñado un nuevo launch wizard de EC2. Para obtener más información, consulte Lance una instancia con el antiguo asistente de inicialización de instancias.	10 de octubre de 2013
Modificación de tipos de instancias reservadas	01/10/201 3	Ahora puede modificar el tipo de instancia reservada de Linux en la misma familia (por ejemplo, M1, M2, M3, C1). Para obtener más información, consulte Modificar instancias reservadas.	09 de octubre de 2013
Modificación de instancias reservadas de Amazon EC2	15/08/201 3	Ahora puede modificar instancias reservadas en una región. Para obtener más información, consulte Modificar instancias reservadas.	11 de septiembr e de 2013
Asignación de una dirección IP pública	15/07/201 3	Ahora puede asignar una dirección IP pública al iniciar una instancia en una VPC. Para obtener más información, consulte Asignar una dirección IPv4 pública durante la inicialización de la instancia.	20 de agosto de 2013
Concesión de permisos de nivel de recursos	15/06/201 3	Amazon EC2 admite nombres de recursos de Amazon (ARN) y claves de condiciones. Para obtener más información, consulte Políticas de IAM para Amazon EC2.	8 de julio de 2013

Característica	Versión de API	Descripción	Fecha de la versión
Copias de instantáneas incrementales	01/02/2013	Ahora puede realizar copias de instantáneas incrementales.	11 de junio de 2013
AWS Management Pack		AWS Management Pack enlaza las instancias de Amazon EC2 con los sistemas operativos Windows o Linux que ejecutan. AWS Management Pack es una extensión de Microsoft System Center Operations Manager.	8 de mayo de 2013
Nueva página Etiquetas		Hay una nueva página Etiquetas en la consola de Amazon EC2. Para obtener más información, consulte Etiquetar los recursos de Amazon EC2.	04 de abril de 2013
Copia de una AMI de una región a otra	01/02/2013	Puede copiar una AMI de una región a otra, lo que le permite iniciar instancias uniformes en más de una región de AWS de una manera rápida y sencilla. Para obtener más información, consulte Copiar una AMI.	11 de marzo de 2013
Inicialización de instancias en una VPC predeterminada	01/02/2013	Su cuenta de AWS puede iniciar instancias en EC2-Classic o en una VPC, o solo en una VPC, según la región. Si solo puede iniciar instancias en una VPC, creamos una VPC predeterminada automáticamente. Cuando lance una instancia, la iniciamos en su VPC predeterminada, a menos que cree una VPC no predeterminada y la especifique al iniciar la instancia.	11 de marzo de 2013

Característica	Versión de API	Descripción	Fecha de la versión
Copia de instantáneas de EBS	01/12/2012	Puede utilizar copias de instantáneas para crear copias de seguridad de los datos, para crear nuevos volúmenes de Amazon EBS o para crear imágenes de máquina de Amazon (AMI).	17 de diciembre de 2012
Métricas de EBS actualizadas y comprobaciones del estado de volúmenes de Provisioned IOPS SSD	01/10/2012	Se han actualizado las métricas de EBS para incluir dos nuevas métricas para volúmenes de Provisioned IOPS SSD. También se han agregado nuevas comprobaciones del estado de volúmenes de Provisioned IOPS SSD.	20 de noviembre de 2012
Estado de solicitud de instancia de spot	01/10/2012	El estado de la solicitud de la instancia de spot ayuda a determinar el estado de las solicitudes de spot.	14 de octubre de 2012
Marketplace de instancias reservadas de Amazon EC2	15/08/2012	El Marketplace de instancias reservadas relaciona a vendedores que tienen instancias reservadas de Amazon EC2 que ya no necesitan con compradores que desean adquirir capacidad adicional. Las instancias reservadas que se compran y se venden en el Marketplace de instancias reservadas funcionan igual que otras instancias reservadas, excepto que les puede quedar menos del plazo estándar completo y se pueden vender a un precio diferente.	11 de septiembre de 2012

Característica	Versión de API	Descripción	Fecha de la versión
Provisioned IOPS SSD para Amazon EBS	20/07/2012	Los volúmenes de Provisioned IOPS SSD ofrecen un rendimiento elevado y predecible en cargas de trabajo que utilizan mucha E/S, como aplicaciones de bases de datos, que se basan en unos tiempos de respuesta rápidos y uniformes.	31 de julio de 2012
Roles de IAM en instancias Amazon EC2	01/06/2012	Los roles de IAM para Amazon EC2 ofrecen: • Claves de acceso a AWS para aplicaciones que se ejecutan en instancias Amazon EC2. • Rotación automática de claves de acceso de AWS en la instancia Amazon EC2. • Permisos detallados para aplicaciones que se ejecutan en instancias Amazon EC2 que realizan solicitudes a los servicios de AWS.	11 de junio de 2012

Característica	Versión de API	Descripción	Fecha de la versión
Características de las instancia de spot que ayudan a comenzar y gestionar el potencial de las interrupciones.		Ahora puede administrar sus instancias de spot de la siguiente forma: • Especifique la cantidad que quiere pagar por instancias de spot utilizando las configura ciones de inicio de Auto Scaling, y configure una programación para especificar la cantidad que quiere pagar por instancias de spot. Para obtener más información, consulte Iniciar instancias de spot en su grupo de Auto Scaling en Guía del usuario de Amazon EC2 Auto Scaling. • Reciba notificaciones cuando se inician o se terminan instancias. • Utilice plantillas de AWS CloudFormation para iniciar instancias de spot en una pila con recursos de AWS.	7 de junio de 2012
Exportación y marcas de tiempo de instancias de EC2 para realizar comprobaciones de estado de Amazon EC2	01/05/2012	Se ha añadido compatibilidad para exportar instancias de Windows Server importadas originalmente en EC2. Se ha añadido compatibilidad para marcas de tiempo en estados de instancias y estados del sistema para indicar la fecha y hora en que falló una comprobación de estado.	25 de mayo de 2012

Característica	Versión de API	Descripción	Fecha de la versión
Exportación de instancias de EC2 y marcas de tiempo en comprobaciones de estado de instancias y el sistema de Amazon VPC	01/05/2012	Se ha añadido compatibilidad para exportar instancias de EC2 a Citrix Xen, Microsoft Hyper-V y VMware vSphere. Se ha añadido compatibilidad con marcas de tiempo en comprobaciones de estado de instancias y el sistema.	25 de mayo de 2012
AMI de AWS Marketplace	01/04/2012	Se ha agregado compatibilidad para las AMI de AWS Marketplace.	19 de abril de 2012
Capas de precios de instancias reservadas	15/12/2011	Se ha añadido una nueva sección en la que se explica cómo utilizar el descuento que se incluye en las capas de precios de instancias reservadas.	5 de marzo de 2012
Interfaces de red elástica (ENI) para instancias de EC2 en Amazon Virtual Private Cloud	01/12/2011	Se ha añadido una nueva sección sobre interfaces de red elásticas (ENI) para instancias de EC2 en una VPC. Para obtener más información, consulte Interfaces de red elásticas.	21 de diciembre de 2011
Nuevos tipos de ofertas para instancias reservadas de Amazon EC2	01/11/2011	Puede elegir entre una gran variedad de ofertas de instancias reservadas diseñadas para el uso que tenga previsto de la instancia.	01 de diciembre de 2011

Característica	Versión de API	Descripción	Fecha de la versión
Estado de la instancia Amazon EC2	01/11/2011	Puede ver detalles adicionales sobre el estado de las instancias, incluidos los eventos programados por AWS que pudieran afectar a las instancias. Estas actividades operativas incluyen los reinicios de instancias que son necesarios para aplicar actualizaciones del software o parches de seguridad, o bien la retirada de instancias que son necesarias cuando hay problemas de hardware. Para obtener más información, consulte Monitorear el estado de las instancias.	16 de noviembre de 2011
Instancias de spot en Amazon VPC	15/07/2011	Se ha añadido información acerca de la compatibilidad con instancias de spot en Amazon VPC. Con esta actualización, los usuarios pueden iniciar instancias de spot en una nube privada virtual (VPC). Al iniciar instancias de spot en un VPC, los usuarios de instancias de spot pueden disfrutar de los beneficios de Amazon VPC.	11 de octubre de 2011
Proceso de VM Import simplificado para los usuarios de herramientas CLI	15/07/2011	El proceso de VM Import se simplifica con la funcionalidad mejorada de `ImportInstance` e `ImportVolume` , que ahora realiza la carga de las imágenes en Amazon EC2 después de crear la tarea de importación. Asimismo, con la introducción de `ResumeImport` , los usuarios pueden reiniciar una carga incompleta en el punto en el que se detuvo la tarea.	15 de septiembre de 2011

Característica	Versión de API	Descripción	Fecha de la versión
Compatibilidad para importar en el formato de archivo VHD		Ahora VM Import puede importar archivos de imagen de máquinas virtuales en formato VHD. El formato de archivo VHD es compatible con las plataformas de virtualización Citrix Xen y Microsoft Hyper-V. En esta versión, VM Import admite ahora los formatos de imagen RAW, VHD y VMDK (compatible con VMware ESX). Para obtener más información, consulte la Guía del usuario de VM Import/Export.	24 de agosto de 2011
Actualización de Amazon EC2 VM Import Connector para VMware vCenter		Se ha añadido información acerca de la versión 1.1 de Amazon EC2 VM Import Connector para el dispositivo virtual VMware vCenter (conector). Esta actualización incluye compatibilidad proxy para el acceso a Internet, se ha mejorado el control de errores y la precisión de la barra de progreso de las tareas y se han solucionado varios errores.	27 de junio de 2011
Cambios en los precios de la zona de disponibilidad de instancias de spot	15/05/2011	Se ha agregado información acerca de la característica de precios de la zona de disponibilidad de instancias de spot. En esta versión, hemos agregado nuevas opciones de precios de la zona de disponibilidad como parte de la información que se recibe cuando se consultan las solicitudes de instancias de spot y el historial de precios de spot. Esto ayuda a determinar el precio necesario para iniciar una instancia de spot en una zona de disponibilidad concreta.	26 de mayo de 2011

Característica	Versión de API	Descripción	Fecha de la versión
AWS Identity and Access Management		Se ha agregado información sobre AWS Identity and Access Management (IAM) que permite a los usuarios especificar las acciones de Amazon EC2 que puede utilizar un usuario con recursos de Amazon EC2 en general. Para obtener más información, consulte Identity and Access Management para Amazon EC2.	26 de abril de 2011
Instancias dedicadas		Las instancias dedicadas, que se inician en Amazon Virtual Private Cloud (Amazon VPC), son instancias que están físicamente aisladas en el nivel de hardware host. Las instancias dedicadas le permiten aprovechar Amazon VPC y la nube de AWS, con la ventaja de que incluye aprovisionamiento elástico bajo demanda y pago solo por lo que usa, además de aislamiento de las instancias informáticas de Amazon EC2 en el nivel de hardware. Para obtener más información, consulte Dedicated Instances.	27 de marzo de 2011
Actualizaciones de instancias reservadas en AWS Management Console		Las actualizaciones en AWS Managemen t Console ayudan a los usuarios a ver sus instancias reservadas y a comprar instancias reservadas adicionales, incluidas las instancias reservadas dedicadas.	27 de marzo de 2011
Información sobre metadatos	01-01-201 1	Se ha añadido información sobre metadatos para reflejar los cambios en la versión del 01/01/2011. Para obtener más información, consulte Trabajar con metadatos de instancias y Categorías de metadatos de instancia.	11 de marzo de 2011

Característica	Versión de API	Descripción	Fecha de la versión
Amazon EC2 VM Import Connector para VMware vCenter		Se ha añadido información acerca de Amazon EC2 VM Import Connector para el dispositivo virtual VMware vCenter (conector). El conector es un complemento de VMware vCenter que se integra con VMware vSphere Client y ofrece una interfaz gráfica de usuario que se puede utilizar para importar las máquinas virtuales de VMware a Amazon EC2.	3 de marzo de 2011
Forzar la separación de volúmenes		Ahora puede utilizar la AWS Management Console para forzar la desconexión de un volumen de Amazon EBS de una instancia.	23 de febrero de 2011
Protección contra la terminación de instancias		Ahora puede utilizar AWS Management Console para evitar que se termine una instancia. Para obtener más información, consulte Cómo habilitar la protección contra la terminación.	23 de febrero de 2011
VM Import	15/11/2010	Se ha añadido información acerca de VM Import, que le permite importar una máquina virtual o un volumen a Amazon EC2. Para obtener más información, consulte la Guía del usuario de VM Import/Export.	15 de diciembre de 2010
Monitorización básica de instancias	31/08/2010	Se ha añadido información acerca de la monitorización básica de instancias de EC2.	12 de diciembre de 2010
Filtros y etiquetas	31/08/2010	Se ha añadido información sobre las listas, los filtros y los recursos de etiquetado. Para obtener más información, consulte Enumerar y filtrar los recursos y Etiquetar los recursos de Amazon EC2.	19 de septiembre de 2010

Característica	Versión de API	Descripción	Fecha de la versión
Lanzamiento de instancias Idempotent	31/08/2010	Se ha añadido información acerca de la forma de garantizar la instancia de idempotencia al ejecutar instancias.	19 de septiembre de 2010
AWS Identity and Access Management para Amazon EC2		Amazon EC2 ahora se integra con AWS Identity and Access Management (IAM). Para obtener más información, consulte Identity and Access Management para Amazon EC2.	2 de septiembre de 2010
Designación de direcciones IP de Amazon VPC	15/06/2010	Ahora los usuarios de Amazon VPC pueden especificar una dirección IP para asignar una instancia iniciada en una VPC.	12 de julio de 2010
Monitoreo de Amazon CloudWatch para volúmenes de Amazon EBS		El monitoreo de Amazon CloudWatch ahora está disponible automáticamente para volúmenes de Amazon EBS.	14 de junio de 2010
Instancias reservadas con Windows		Ahora Amazon EC2 es compatible con instancias reservadas con Windows	22 de febrero de 2010