Guía de introducción

AWS Management Console

Version 1.0

AWS Management Console: Guía de introducción

Table of Contents

¿Qué es el AWS Management Console?

AWS Management ConsoleSe trata de una aplicación web que comprende y hace referencia a una amplia colección de consolas de servicio para gestionar AWS los recursos. La primera vez que inicie sesión, verá la página de inicio de la consola. La página de inicio proporciona acceso a la consola de cada servicio y ofrece un único lugar para acceder a la información que necesita para realizar sus tareas relacionadas a AWS . También te permite personalizar la experiencia de Console Home añadiendo, quitando y reorganizando widgets como Visitas recientes, AWS Salud y más.

> **Note**
>
> La opción de selección de idioma se ha movido a la nueva página de configuración unificada. Para obtener más información, consulte Cambio del idioma de la AWS Management Console.

Por otro lado, las consolas de servicios individuales ofrecen una amplia gama de herramientas para la computación en la nube, así como información sobre su cuenta y sobre facturación.

Uso del dispositivo de su elección

La AWS Management Console se ha diseñado para funcionar en tabletas, así como en otros tipos de dispositivos:

- El espacio vertical y horizontal se maximiza para que quepa más en la pantalla.

- Los botones y selectores son mayores para una mejor experiencia táctil.

También AWS Management Console está disponible como aplicación para Android e iOS. Esta aplicación permite realizar tareas pertinentes en dispositivos móviles, las cuales mejoran la experiencia total en la web. Por ejemplo, puede ver y gestionar fácilmente sus instancias Amazon EC2 y CloudWatch alarmas de Amazon existentes desde su teléfono.

Puedes descargar la aplicación móvil de la AWS consola desde Amazon Appstore, Google Play o iTunes.

Configuración del AWS Management Console

En este tema se describe cómo configurar la página de configuración unificada AWS Management Console y cómo utilizarla para establecer los valores predeterminados que se aplican a todas las consolas de servicio. También se explican los widgets, una función del panel principal de la consola que permite añadir componentes personalizados que permiten realizar un seguimiento de la información sobre sus AWS servicios y recursos.

Temas

Trabajar con widgets

El panel de control de Console Home incluye widgets que muestran información importante sobre su AWS entorno y proporcionan accesos directos a sus servicios. Puede personalizar la experiencia agregando y eliminando widgets, reorganizándolos o cambiando su tamaño.

Para agregar un widget

1. En la parte superior o inferior derecha del panel de inicio de la consola, elija el botón +Agregar widgets.
2. Elija el indicador de arrastre, representado por seis puntos verticales en la parte superior izquierda de la barra de título del widget y arrástrelo al panel de inicio de la consola.

Para eliminar un widget

1. Elija los puntos suspensivos, representados por tres puntos verticales en la parte superior derecha de la barra de título del widget.
2. Elija Remove widget (Eliminar widget).

Para reorganizar los widgets

- Elija el indicador de arrastre, representado por seis puntos verticales en la parte superior izquierda de la barra de título del widget y arrastre el widget hasta una nueva ubicación en el panel de inicio de la consola.

Para cambiar el tamaño de un widget

- Elija el icono de cambio de tamaño en la parte inferior derecha del widget y, a continuación, arrastre el widget para cambiar de tamaño.

Si quiere empezar de nuevo organizando y configurando los widgets, puede restablecer el panel de inicio de la consola al diseño predeterminado. Esto revertirá los cambios en el diseño del panel de inicio de la consola y restaurará todos los widgets a la ubicación y el tamaño predeterminados.

Para restablecer la página al diseño predeterminado

1. Elija el botón Restablecer al diseño predeterminado en la parte superior derecha de la página.
2. Para confirmar, seleccione Restablecer.

> **Note**
>
> Esto revertirá todos los cambios en el diseño del panel de inicio de la consola.

Para solicitar un nuevo widget en el panel de inicio de la consola

1. En la esquina inferior izquierda del panel de inicio de la consola, elija ¿Desea ver otro widget? ¡Díganos!

   Describa el widget que desea ver agregado al panel de inicio de la consola.
2. Seleccione Submit (Enviar).

> **Note**
>
> Las sugerencias se revisan periódicamente y es posible que se añadan nuevos widgets en futuras actualizaciones de la AWS Management Console.

Establecimiento de la configuración unificada

Puede configurar los ajustes y los valores predeterminados, como la pantalla, el idioma y la región, desde la página de configuración AWS Management Console unificada. El modo visual y el idioma predeterminado también se pueden definir directamente desde la barra de navegación. Estos cambios se aplican a todas las consolas de servicio.

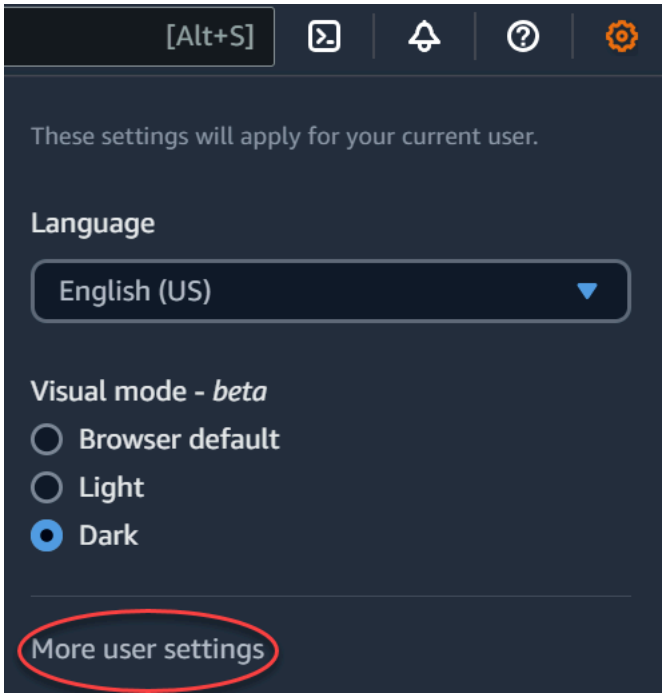
> **Important**
>
> Para garantizar que tu configuración, tus servicios favoritos y los servicios visitados recientemente se conserven en todo el mundo, estos datos se almacenan en todos los sitios Regiones de AWS, incluidas las regiones que están deshabilitadas de forma predeterminada. Estas regiones son África (Ciudad del Cabo), Asia-Pacífico (Hong Kong), Asia-Pacífico (Hyderabad), Asia-Pacífico (Yakarta), Europa (Milán), Europa (España), Europa (Zúrich), Medio Oriente (Baréin) y Medio Oriente (Emiratos Árabes Unidos). Todavía tiene que habilitar manualmente una región para acceder a ella y, a continuación, crear y administrar recursos en esa región. Si no quieres almacenar todos estos datos Regiones de AWS, selecciona Restablecer todo para borrar la configuración y, a continuación, opta por no recordar los servicios visitados recientemente en la administración de ajustes.

Acceder a la configuración unificada

El siguiente procedimiento describe cómo acceder a la configuración unificada.

Para acceder a la configuración unificada

1. Inicie sesión en la AWS Management Console.
2. En la barra de navegación, seleccione el icono de engranaje.
3. Para abrir la página Configuración unificada, elija Más configuración de usuarios.



Restablecer la configuración unificada

Puede eliminar todas las configuraciones de los ajustes unificados y restaurar los ajustes predeterminados restableciendo los ajustes unificados.

> **Note**
>
> Esto afecta a varias áreas AWS, como los servicios favoritos en la navegación y el menú Servicios, los servicios visitados recientemente en los widgets de inicio de la consola y en la consola AWS Console Mobile Application, y todos los ajustes que se aplican a todos los servicios, como el idioma predeterminado, la región predeterminada y el modo visual.

Para restablecer todos los ajustes unificados

1. Inicie sesión en la AWS Management Console.
2. En la barra de navegación, selecciona el icono de engranaje.
3. Abra la página de configuración unificada seleccionando Más configuraciones de usuario.
4. Seleccione Restablecer todo.

Edición de la configuración unificada

El siguiente procedimiento describe cómo editar la configuración preferida.

Para editar la configuración unificada

1. Inicie sesión en la AWS Management Console.
2. En la barra de navegación, selecciona el icono de engranaje.
3. Abra la página de configuración unificada seleccionando Más configuraciones de usuario.
4. Elija Edit (Editar) junto a la configuración que prefiera:

   - Localization and default Region (Localización y región predeterminada):
     - Idioma le permite seleccionar el idioma predeterminado para el texto de la consola.
     - Default Region (Región predeterminada) le permite seleccionar una región predeterminada que se aplica cada vez que se conecta. Puede seleccionar cualquiera de las regiones disponibles para su cuenta. También puede seleccionar la última región utilizada como predeterminada.

       Para obtener más información sobre el enrutamiento de las regiones en la AWS Management Console, consulte Elección de una región.
   - Display (Visualización):
     - El Visual mode (Modo visual) le permite configurar la consola en modo claro, modo oscuro o modo de visualización predeterminado del navegador.

       El modo oscuro es una característica beta y es posible que no se aplique en todas las consolas de servicio de AWS .
     - Visualización de la barra Favoritos alterna la visualización de la barra Favoritos entre el nombre completo del servicio con su icono o solo el icono del servicio.
     - El tamaño del icono de la barra de favoritos cambia el tamaño del icono del servicio en la pantalla de la barra de favoritos entre pequeño (16x16 píxeles) y grande (24x24 píxeles).
   - Settings management (Administración de la configuración):
     - Recordar los servicios visitados recientemente le permite elegir si desea AWS Management Console recordar los servicios visitados recientemente. Si lo desactivas, también se borra el historial de los servicios visitados recientemente, por lo que ya no verás los servicios visitados recientemente en el menú de servicios ni en los widgets de la página de inicio de la consola. AWS Console Mobile Application

5. Elija Guardar cambios.

Cambia el modo visual de AWS Management Console

El modo visual configura la consola en modo claro, modo oscuro o el modo de visualización predeterminado del navegador.

Para cambiar el modo visual desde la barra de navegación

1. Inicie sesión en la AWS Management Console.
2. En la barra de navegación, selecciona el icono con forma de engranaje.
3. En Modo visual, elija Claro para el modo claro, Oscuro para el modo oscuro o Predeterminado del navegador para el modo de visualización predeterminado del navegador.

Cambiar el idioma predeterminado en la configuración unificada

El siguiente procedimiento describe cómo cambiar el idioma predeterminado mediante la barra de navegación.

Para cambiar el idioma predeterminado de la barra de navegación

1. Inicie sesión en la AWS Management Console.
2. En la barra de navegación, seleccione el icono de engranaje.
3. En Idioma, elija el idioma Predeterminado del navegador o el preferido de la lista desplegable.

Selección de una región

Para muchos servicios, puede elegir uno Región de AWS que especifique dónde se administran los recursos. Las regiones son conjuntos de AWS recursos ubicados en la misma área geográfica. No es necesario que elijas una región para los servicios AWS Management Consoleo algunos de ellos, como AWS Identity and Access Management. Para obtener más información sobre Regiones de AWS, consulte Managing Regiones de AWS (Administración de Regiones de AWS) en la Referencia general de AWS.

Para elegir una región

1. Inicie sesión en la AWS Management Console.

2. Elija un servicio para ir a la consola de dicho servicio.
3. En la barra de navegación, elija el nombre de la región que aparece. A continuación, elija la región a la que desea cambiar.

Para elegir una región predeterminada

1. En la barra de navegación, elija el icono de configuración y, a continuación, elija Más configuración de usuarios para ir a la página Configuración unificada.
2. Elija Edit (Editar) junto a Localization and default Region (Localización y región predeterminada).
3. Selecciona tu región predeterminada y, a continuación, selecciona Guardar configuración. Si no selecciona una región predeterminada, la última región que haya visitado será la predeterminada.
4. (Opcional) Selecciona Ir a la nueva región predeterminada para ir inmediatamente a la nueva región predeterminada.

> **Note**
>
> Si ha creado AWS recursos pero no los ve en la consola, es posible que la consola muestre recursos de otra región. Algunos recursos (como las instancias de Amazon EC2) son específicos de la región en que se han creado. Para verlos, utilice el selector de región para elegir la región que contiene sus recursos.

Cómo agregar y eliminar favoritos

Para acceder más rápidamente a los servicios de uso frecuente, puede guardar las consolas de servicio en una lista de Favorites (Favoritos).

Agregar un servicio a la lista de Favorites (Favoritos)

1. Inicie sesión en la AWS Management Console.
2. Elija el botón Add widgets (Agregar widgets) en la parte superior o inferior derecha de la página.
3. En el menú Agregar widgets, seleccione los Favoritos que desea añadir a la consola y, a continuación, elija Agregar.

Los favoritos se añaden a la parte inferior de la página de inicio de su consola. Para arrastrar y soltar favoritos, seleccione la barra de título en la parte superior del widget y, a continuación, arrastre el widget a una nueva ubicación en la página.

4. En la barra de navegación, elija Services (Servicios).
5. En la lista de servicios Visitados recientemente o en la lista Todos los servicios, pase el ratón sobre el nombre del servicio que desea añadir como favorito.
6. Seleccione la estrella situada a la izquierda del nombre del servicio.
7. Repita los dos pasos anteriores para agregar más servicios a su lista de Favorites (Favoritos).

Eliminar un servicio de la lista de Favorites (Favoritos)

1. En la barra de navegación, elija Services (Servicios).
2. Realice una de las siguientes acciones siguientes:

   - En la lista de Favoritos, sitúese sobre el nombre de un servicio. A continuación, elija la opción x a la derecha del nombre del servicio.
   - En la lista de servicios Recently visited (Visitados recientemente) o en la lista de All services (Todos los servicios), anule la selección de la estrella junto al nombre de un servicio que esté en su lista de Favorites (Favoritos).

Cómo cambiar la contraseña

Si es propietario de una cuenta, puede cambiar la contraseña de la AWS cuenta desde AWS Management Console.

Para cambiar su contraseña de

1. Inicie sesión en la AWS Management Console.
2. En la barra de navegación, elija el nombre de la cuenta.
3. Elija Security Credentials (Credenciales de seguridad).
4. Las opciones que se muestran variarán en función del Cuenta de AWS tipo. Siga las instrucciones que se muestran en la consola para cambiar la contraseña.
5. Ingrese su contraseña actual una vez y la contraseña nueva dos veces.

   La contraseña nueva debe tener al menos ocho caracteres y debe incluir lo siguiente:

- Al menos un símbolo
- Al menos un número
- Al menos una letra mayúscula
- Al menos una letra minúscula

6. Elija Change Password (Cambiar contraseña) o Save changes (Guardar cambios).

Cambiar el idioma del AWS Management Console

La AWS Console Home experiencia incluye la página de configuración unificada, donde puede cambiar el idioma predeterminado de AWS los servicios del AWS Management Console. También puede cambiar el idioma predeterminado rápidamente desde el menú de configuración, al que puede acceder desde la barra de navegación. Puedes realizar esta modificación desde cualquier lugar de la consola.

> **Note**
>
> Este procedimiento cambia el idioma de todas las consolas, pero no el de la documentación de AWS . Para cambiar el idioma empleado en la documentación, utilice el menú de idioma situado en la esquina superior derecha de cualquier página de documentación.

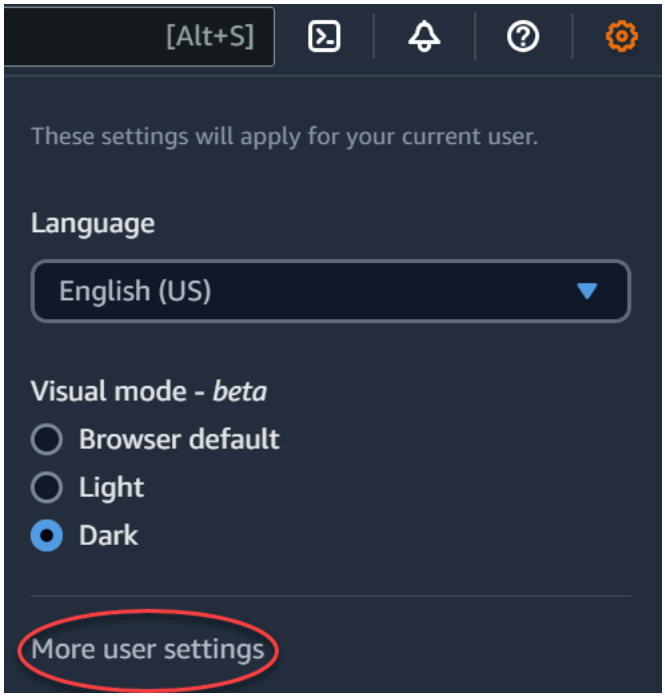
AWS Management Console Actualmente, es compatible con los siguientes idiomas:

- English (EE. UU.)
- Inglés (Reino Unido)
- Bahasa Indonesia
- Alemán
- Francés
- Japonés
- Español
- Italiano
- Portugués
- Coreano
- Chino simplificado

- Chino tradicional

Para cambiar el idioma predeterminado en la configuración unificada

1. Inicie sesión en la AWS Management Console.
2. En la barra de navegación, elija el icono de configuración.
3. Para abrir la página Configuración unificada, elija Más configuración de usuarios.



4. En Unified Settings (Configuración unificada), elija Edit (Editar) junto a Localization and default Region (Localización y región predeterminada).
5. Para seleccionar el idioma que desea para la consola, elija una de las siguientes opciones:

   - Elija el Navegador predeterminado en la lista desplegable y, a continuación, seleccione Guardar configuración.

     El texto de la consola para todos los AWS servicios aparece en el idioma que prefieras y que hayas establecido en la configuración del navegador.

     > **Note**
     >
     > El navegador predeterminado solo admite los idiomas que admite la AWS Management Console.

- Elija el idioma que prefiera en la lista desplegable y, a continuación, seleccione Guardar configuración.

  El texto de la consola para todos los AWS servicios aparece en el idioma que prefieras.

Para cambiar el idioma predeterminado de la barra de navegación

1. Inicie sesión en la AWS Management Console.
2. En la barra de navegación, elija el icono de configuración.
3. En Idioma, elija el idioma Predeterminado del navegador o el preferido de la lista desplegable.

Introducción a un servicio

La AWS Management Console ofrece varias formas para navegar a las distintas consolas de servicios.

Para abrir una consola de servicio

Realice alguna de las siguientes acciones:

- En el cuadro de búsqueda de la barra de navegación, ingrese el nombre completo o parcial del servicio. A continuación, en Services, (Servicios), elija el servicio que desee de la lista de resultados de la búsqueda. Para obtener más información, consulte Búsqueda de productos, servicios, funciones y mucho más mediante la búsqueda unificada .
- En el widget Recently visited services (Servicios visitados recientemente), elija un nombre de servicio.
- En el widget Recently visited services (Servicios visitados recientemente), elige View all AWS services (Ver todos los servicios de AWS). Después, en la página All AWS services (Todos los servicios de AWS, elige un nombre de servicio.
- En la barra de navegación elija Services (Servicios) para abrir una lista completa de los servicios. A continuación, elija un servicio en Recently visited (Recientemente visitados) o All services (Todos los servicios).

Búsqueda de productos, servicios, funciones y mucho más mediante la búsqueda unificada

El cuadro de búsqueda de la barra de navegación ofrece una herramienta de búsqueda unificada para localizar servicios y características de AWS , documentación de servicios y de AWS Marketplace. Basta con teclear algunos caracteres para ver los resultados de todas estas categorías. Cuantos más caracteres escriba, más se refinan los resultados de la búsqueda.

Para buscar un servicio, una función, una documentación o un AWS Marketplace producto

1. En el cuadro de búsqueda de la barra de navegación del AWS Management Console, introduzca todos o parte de los términos de búsqueda.
2. Para refinar su búsqueda y obtener más detalles, realice cualquiera de las siguientes acciones:
   - Para limitar los resultados al tipo de contenido deseado, elija una de las categorías de la izquierda.
   - Para ver más resultados de una categoría determinada, elija See all ***n*** results (Ver todos los n resultados) por cada encabezamiento de categoría. Para volver a la lista principal de resultados, elija Back (Atrás) en la esquina superior izquierda.
   - Para navegar rápidamente a las características más populares de un servicio, sitúese sobre el nombre del servicio en los resultados y elija un enlace.
   - Para obtener más detalles sobre una documentación o un AWS Marketplace resultado, haga una pausa en el título del resultado.
3. Elija cualquier enlace para navegar al servicio, tema o página de AWS Marketplace que desee.

> **Tip**
>
> También puede utilizar el teclado para navegar rápidamente hasta el primer resultado de búsqueda. En primer lugar, pulse Alt+s (Windows) o Opción+s (macOS) para acceder a la barra de búsqueda. A continuación, comience a introducir el término de búsqueda. Cuando el resultado deseado aparezca en la parte superior de la lista, pulse Enter (Intro). Por ejemplo, para navegar rápidamente a la consola de Amazon EC2, ingrese ec2 y, a continuación, pulse Enter (Intro).

Chatea con un desarrollador de Amazon Q

Amazon Q Developer es un asistente conversacional basado en inteligencia artificial (IA) generativa que puede ayudarlo a comprender, crear, ampliar y operar AWS aplicaciones. Puede hacer cualquier pregunta a Amazon Q AWS, incluidas preguntas sobre la AWS arquitectura, sus AWS recursos, las prácticas recomendadas, la documentación y mucho más. También puede crear casos de soporte y recibir asistencia de un agente en vivo. Para obtener más información, consulta ¿Qué es Amazon Q? en la Guía del usuario para desarrolladores de Amazon Q.

Empieza a usar Amazon Q

Para empezar a chatear con Amazon Q en los sitios web de AWS documentación AWS Management Console, en los sitios AWS web o en la aplicación AWS Console Mobile Application, selecciona el icono hexagonal de Amazon Q. Para obtener más información, consulte Introducción a Amazon Q Developer en la Guía del usuario para desarrolladores de Amazon Q.

Preguntas de ejemplo

Los siguientes son algunos ejemplos de preguntas que puedes hacerle a Amazon Q:

- `How do I get billing support?`
- `How do I create an EC2 instance?`
- `How do I troubleshoot a "Failed to load" error?`
- `How do I close an AWS account?`
- `Can you connect me with a person?`

¿En qué está MyApplications? AWS

myApplications es una extensión del inicio de la consola que le ayuda a administrar y monitorear el costo, el estado, la posición de seguridad y el rendimiento de las aplicaciones en AWS. Puede acceder a todas las aplicaciones de su cuenta, a las métricas clave de todas las aplicaciones y a una visión general de las métricas e información sobre costes, seguridad y operaciones de varias consolas de servicio desde una sola vista en la AWS Management Console. myApplications incluye lo siguiente:

- El widget de aplicaciones está en la página de inicio de la consola
- myApplications que puede usar para ver los costos de los recursos de las aplicaciones y los resultados de seguridad
- Panel de myApplications que proporciona una vista de las métricas clave de las aplicaciones como los costos, el rendimiento y los resultados de seguridad

Características de myApplications

- Crear aplicaciones: cree nuevas aplicaciones y organice los recursos. Sus aplicaciones se muestran automáticamente en MyApplications, por lo que puede realizar acciones en las API AWS Management Console, la CLI y los SDK. La infraestructura como código (IaC) se genera al crear una aplicación y se puede acceder a ella desde el panel de myApplication. El iaC se puede utilizar en las herramientas de iAC, como Terraform. AWS CloudFormation
- Acceder a las aplicaciones: puede acceder rápidamente a cualquiera de las aplicaciones desde el widget de myApplications seleccionándolo.
- Comparar las métricas de las aplicaciones: utilice myApplications para comparar las métricas clave de las aplicaciones, como el costo de los recursos de las aplicaciones y la cantidad de resultados de seguridad críticos para varias aplicaciones.
- Supervise y gestione las aplicaciones: evalúe el estado y el rendimiento de las aplicaciones mediante alarmas, parámetros y objetivos de nivel de servicio a partir de Amazon CloudWatch los resultados obtenidos y las tendencias de AWS Security Hub costes. AWS Cost Explorer Service También puede encontrar resúmenes y optimizaciones de métricas informáticas y gestionar el cumplimiento de los recursos y el estado de la configuración desde. AWS Systems Manager

Servicios relacionados

myApplications utiliza los siguientes servicios:

- AppRegistry
- AppManager
- Amazon CloudWatch
- Amazon EC2
- AWS Lambda
- Explorador de recursos de AWS
- AWS Security Hub
- Systems Manager
- AWS Service Catalog
- Etiquetado

Acceso a myApplications

Puede acceder a myApplications desde la AWS Management Console eligiendo myApplications en la barra lateral izquierda.

Precios

MyApplications on AWS se ofrece sin coste adicional. No se requieren pagos de configuración ni compromisos iniciales. Los cargos por el uso de los recursos y servicios subyacentes que resume el panel de control de myApplication se siguen aplicando a las tarifas publicadas para esos recursos.

Regiones admitidas

MyApplications está disponible en las siguientes direcciones: Regiones de AWS

- US East (Ohio)
- Este de EE. UU. (Norte de Virginia)
- Oeste de EE. UU. (Norte de California)

- Oeste de EE. UU. (Oregón)
- Asia-Pacífico (Bombay)
- Asia-Pacífico (Osaka)
- Asia-Pacífico (Seúl)
- Asia-Pacífico (Singapur)
- Asia-Pacífico (Sídney)
- Asia-Pacífico (Tokio)
- Canadá (centro)
- Europa (Fráncfort)
- Europa (Irlanda)
- Europa (Londres)
- Europa (París)
- Europa (Estocolmo)
- América del Sur (São Paulo)

Regiones registradas

Las regiones de suscripción no están habilitadas de forma predeterminada. Debe habilitar estas regiones manualmente para poder usarlas con myApplications. Para obtener más información al respecto Regiones de AWS, consulte Administración Regiones de AWS. Solo se admiten las siguientes regiones registradas:

- África (Ciudad del Cabo)
- Asia-Pacífico (Hong Kong)
- Asia-Pacífico (Hyderabad)
- Asia-Pacífico (Yakarta)
- Asia-Pacífico (Melbourne)
- Europa (Milán)
- Europa (España)
- Europa (Zúrich)
- Medio Oriente (Baréin)

- Medio Oriente (EAU)
- Israel (Tel Aviv)

Introducción a myApplications

Para empezar a utilizar myApplications para crear, monitorear y administrar las aplicaciones, siga los siguientes pasos.

Paso 1: Crear una aplicación

Cree una nueva aplicación o incorpore una AppRegistry aplicación existente creada antes del 8 de noviembre de 2023 para empezar a utilizar MyApplications.

Create an application

Para crear una aplicación

1. Inicie sesión en la AWS Management Console.
2. En la barra lateral izquierda, elija myApplications.
3. Elija Crear aplicación.
4. Ingrese un nombre de aplicación.
5. (Opcional) Escriba una descripción para la aplicación.
6. (Opcional) Agregue etiquetas. Las etiquetas son pares clave-valor que se aplican a los recursos para almacenar metadatos sobre estos recursos.

   > **Note**
   >
   > La etiqueta de la AWS aplicación se aplica automáticamente a las aplicaciones recién creadas y se puede utilizar para identificar los recursos asociados a la aplicación. Para obtener más información, consulte La etiqueta de la AWS aplicación en la Guía AWS Service Catalog AppRegistry del administrador.

7. (Opcional) Agregue grupos de atributos. Puede usar grupos de atributos para almacenar los metadatos de la aplicación.
8. Elija Siguiente.
9. (Opcional) Agregue los recursos existentes:

> **Note**
>
> Para buscar y agregar recursos, debe activar Explorador de recursos de AWS. Para obtener más información, consulte Primeros pasos con Explorador de recursos de AWS.
> Todos los recursos agregados se etiquetan con la etiqueta de AWS aplicación.

a. Elija Seleccionar recursos.

b. (Opcional) Elija una vista.

c. Busque los recursos. Puede buscar por palabra clave, nombre o tipo, o elegir un tipo de recurso.

> **Note**
>
> Si no puede encontrar el recurso que busca, solucione el problema con Explorador de recursos de AWS. Para obtener más información, consulte Solución de problemas de búsqueda de Resource Explorer en la Guía del usuario de Resource Explorer.

d. Seleccione la casilla de verificación junto a los recursos que desee agregar.

e. Seleccione Añadir.

f. Elija Siguiente.

10. Revise las opciones.

11. Si vas a asociar una AWS CloudFormation pila, selecciona la casilla de verificación situada en la parte inferior de la página.

> **Note**
>
> Para añadir una AWS CloudFormation pila a la aplicación es necesario actualizar la pila, ya que todos los recursos que se añaden a la aplicación se etiquetan con la etiqueta de AWS aplicación. Es posible que las configuraciones manuales realizadas después de la última actualización de la pila no se reflejen después de esta actualización. Esto puede provocar tiempos de inactividad u otros problemas con las aplicaciones. Para obtener más información, consulte Comportamientos

de actualización de los recursos de la pila en la Guía del usuario de AWS CloudFormation .

12. Elija Crear aplicación.

Onboard existing application

Para incorporar una AppRegistry aplicación existente

1. Inicie sesión en la AWS Management Console.
2. En la barra lateral izquierda, elija myApplications.
3. Use la barra de búsqueda para encontrar la aplicación.
4. Seleccione la aplicación.
5. Elija el ***nombre de la aplicación*** integrada.
6. Si va a asociar una CloudFormation pila, seleccione la casilla de verificación del cuadro de alerta.
7. Elija la aplicación integrada.

Paso 2: Visualización de aplicaciones

Puede consultar las solicitudes en todas las regiones o en regiones específicas y la información relevante en forma de tarjeta o tabla.

Para ver aplicaciones

1. En la barra lateral izquierda, elija myApplications.
2. En Regiones, seleccione Región actual o Regiones admitidas.
3. Para encontrar una aplicación específica, ingrese su nombre, palabras clave o descripción en la barra de búsqueda.
4. (Opcional) La vista predeterminada es la vista de tarjeta. Para personalizar la página de la aplicación:
   a. Seleccione el icono de engranaje.
   b. (Opcional) Seleccione el tamaño de la página.
   c. (Opcional) Elija una vista de tarjeta o de tabla.

d. (Opcional) Seleccione el tamaño de la página.

e. (Opcional) Si utiliza la vista de tabla, seleccione las propiedades de la vista de tabla.

f. (Opcional) Cambie las propiedades de la aplicación que están visibles y el orden en que aparecen.

g. Elija Confirmar.

Administración de aplicaciones

En este tema se explica cómo puede administrar las aplicaciones.

Edición de aplicaciones

Al editar la aplicación AppRegistry , se abre para que pueda actualizar su descripción. También se puede utilizar AppRegistry para editar las etiquetas y los grupos de atributos de la aplicación.

Para editar una aplicación

1. Abra la AWS Management Console.
2. En la barra lateral izquierda de la consola, elija myApplications.
3. Seleccione la aplicación que desee editar.
4. En el panel de myApplication, elija Acciones y, a continuación, elija Editar aplicación.
5. En Editar la descripción de la aplicación, actualice la descripción y, a continuación, elija Guardar cambios.

Para editar etiquetas

- Siga los pasos de Administración de etiquetas de la Guía AWS Service Catalog AppRegistry del administrador.

Para editar grupos de atributos

- Siga los pasos de Edición de grupos de atributos de la Guía AWS Service Catalog AppRegistry del administrador.

Eliminación de aplicaciones

Puede eliminar aplicaciones si ya no son necesarias.

Eliminación de una aplicación

1. Abra la AWS Management Console.
2. En la barra lateral izquierda de la consola, elija myApplications.
3. Seleccione la aplicación que desea eliminar.
4. En el panel de myApplication, elija Acciones.
5. Seleccione Eliminar aplicación.
6. Elija Eliminar.
7. Confirme la eliminación y luego elija Eliminar aplicación.

Creación de fragmentos de código

myApplications crea fragmentos de código para todas las aplicaciones. Puede usar fragmentos de código para agregar automáticamente los recursos recién creados a una aplicación mediante las herramientas de infraestructura como código (IaC). Todos los recursos añadidos se etiquetan con la etiqueta de la AWS aplicación para asociarla a la aplicación.

Para crear un fragmento de código para la aplicación

1. Abra la AWS Management Console.
2. En la barra lateral izquierda de la consola, elija myApplications.
3. Busque y seleccione una aplicación.
4. Elija Actions.
5. Elija Obtener fragmento de código.
6. Seleccione un tipo de fragmento de código.
7. Elija Copiar para copiar el código en el portapapeles.
8. Pegue el código en la herramienta iAC.

Administración de recursos

En este tema se explica cómo administrar los recursos.

Agregar recursos

Agregar recursos a las aplicaciones le permite agruparlas y administrar su seguridad, rendimiento y conformidad.

Para agregar recursos

1. Abra la AWS Management Console.
2. En la barra lateral izquierda de la consola, elija myApplications.
3. Busque y seleccione una aplicación.
4. Elija Administrar recursos.
5. Elija Agregar recursos.
6. (Opcional) Elija una vista.
7. Busque los recursos. Puede buscar por palabra clave, nombre o tipo, o elegir un tipo de recurso.

> **Note**
>
> Si no puede encontrar el recurso que busca, solucione el problema con. Explorador de recursos de AWS Para obtener más información, consulte Solución de problemas de búsqueda de Resource Explorer en la Guía del usuario de Resource Explorer.

8. Seleccione la casilla de verificación junto a los recursos que desee agregar.
9. Elija Añadir.

Eliminación de recursos

Puede eliminar recursos para anular la asociación de la aplicación.

Para eliminar recursos

1. Abra la AWS Management Console.
2. En la barra lateral izquierda de la consola, elija myApplications.
3. Busque y seleccione una aplicación.
4. Elija Administrar recursos.
5. (Opcional) Elija una vista.

6. Busque los recursos. Puede buscar por palabra clave, nombre o tipo, o elegir un tipo de recurso.

> **Note**
>
> Si no puede encontrar el recurso que busca, solucione el problema con. Explorador de recursos de AWS Para obtener más información, consulte Solución de problemas de búsqueda de Resource Explorer en la Guía del usuario de Resource Explorer.

7. Elija Eliminar.
8. Confirme que desea eliminar el recurso eligiendo Eliminar recursos.

Panel de myApplications

Cada aplicación que cree o incorpore tiene su propio panel de myApplications. El panel de control de MyApplications contiene widgets de costes, seguridad y operaciones que permiten obtener información sobre varios AWS servicios. Cada widget también se puede marcar como favorito, reordenar, eliminar o cambiar su tamaño. Para obtener más información, consulte Trabajar con widgets.

Widget de configuración del panel de aplicaciones

Este widget contiene una lista de actividades de introducción sugeridas que puede utilizar como ayuda Servicios de AWS para configurar la administración de los recursos de las aplicaciones.

Widget de resumen de aplicaciones

Este widget muestra el nombre, la descripción y la etiqueta de la aplicación de AWS para la aplicación. Puede acceder a la etiqueta de la aplicación y copiarla en Infraestructura como código (IaC) para etiquetar los recursos manualmente.

Widget informático

Este widget muestra información y métricas de los recursos informáticos que se agregan a la aplicación. Esto incluye el total de alarmas y los tipos totales de recursos informáticos. El widget también muestra gráficos de tendencias de las métricas de rendimiento de los recursos Amazon CloudWatch para la utilización de la CPU de las instancias Amazon EC2 y las invocaciones a Lambda.

Configuración del widget informático

Para rellenar los datos en el widget informático, configure al menos una instancia de Amazon EC2 o una función de Lambda para la aplicación. Para obtener más información, consulte la documentación de Amazon Elastic Compute Cloud e Introducción a Lambda en la Guía para desarrolladores de AWS Lambda .

Widget de costo y uso

Este widget muestra los datos de AWS costo y uso de los recursos de su aplicación. Puede usar estos datos para comparar los costos mensuales y ver los desgloses de los costos de Servicio de AWS. Este widget solo resume los costos de los recursos etiquetados con la etiqueta de AWS aplicación, sin incluir los impuestos, tasas y otros costos compartidos que no estén directamente asociados a un recurso. Los costos mostrados no están combinados y se actualizan al menos una vez cada 24 horas. Para obtener más información, consulte Análisis de los costos con Explorador de recursos de AWS en la Guía del usuario de AWS Cost Management .

Configuración del widget de costo y uso

Para configurar el widget de costo y uso, habilítelo AWS Cost Explorer Service para su aplicación y su cuenta. Este servicio se ofrece sin cargo adicional y no hay tarifas de configuración ni compromiso por adelantado. Para obtener más información, consulte Habilitar Cost Explorer en la Guía del usuario de AWS Cost Management .

AWS Widget de seguridad

Este widget muestra los resultados de AWS seguridad de su aplicación. AWS La seguridad proporciona una visión completa de los hallazgos de seguridad de su aplicación en AWS. Puede acceder a los resultados prioritarios recientes por gravedad, monitorear la posición de seguridad, acceder a los resultados críticos o de gravedad alta recientes y obtener información para los próximos pasos. Para obtener más información, consulte AWS Security Hub.

Configuración del widget AWS de seguridad

Para configurar el widget AWS de seguridad, configúrelo AWS Security Hub para su aplicación y su cuenta. Para obtener más información, consulte ¿Qué es AWS Security Hub? en la Guía AWS Security Hub del usuario. Para obtener información sobre los precios, consulte la versión de prueba gratuita de AWS Security Hub , el uso y los precios en la Guía del usuario de AWS Security Hub .

AWS Security Hub requiere que configure AWS Config Recording. Este servicio proporciona una vista detallada de los recursos asociados a su AWS cuenta. Para obtener más información, consulte AWS Systems Manager en la Guía del usuario de AWS Systems Manager .

DevOps widget

Este widget muestra información operativa para que pueda evaluar el cumplimiento y tomar medidas para la aplicación. Estos datos incluyen:

- Administración de flotas
- Administración de estados
- Administración de parches
- Configuración y OpsItems administración

Configuración del DevOps widget

Para configurar el DevOps widget, actívelo AWS Systems Manager OpsCenter para su aplicación y su cuenta. Para obtener más información, consulte Introducción a Systems Manager Explorer y OpsCenter en la Guía del AWS Systems Manager usuario. OpsCenter La activación AWS Systems Manager Explorer permite configurar AWS Config y hacer Amazon CloudWatch que sus eventos se creen automáticamente en OpsItems función de las reglas y eventos más utilizados. Para obtener más información, consulte Configuración OpsCenter en la Guía del AWS Systems Manager usuario.

Puede configurar las instancias para que los agentes de Systems Manager se ejecuten y apliquen permisos para habilitar el escaneo de parches. Para obtener más información, consulte Configuración rápida de AWS Systems Manager en la Guía del usuario de AWS Systems Manager .

También puede configurar la aplicación de parches automática para las instancias de Amazon EC2 mediante la AWS Systems Manager configuración de Patch Manager. Para obtener más información, consulte Uso de las políticas de parches de configuración rápida en la Guía del usuario de AWS Systems Manager .

Para obtener información sobre los precios, consulte Precios de AWS Systems Manager.

Widget de monitoreo y operaciones

Este widget muestra:

- Alarmas y alertas de los recursos asociados a la aplicación

- Métricas y objetivos del nivel de servicio (SLO) de la aplicación
- Métricas de AWS Application Signals disponibles

Configuración del widget de monitoreo y operaciones

Para configurar el widget de monitoreo y operaciones, cree CloudWatch alarmas y canarios en su AWS cuenta. Para obtener más información, consulta Cómo usar CloudWatch las alarmas de Amazon y Crear un canario en la Guía del CloudWatch usuario de Amazon. Para ver los precios CloudWatch alarmantes y sintéticos, consulta los CloudWatch precios de Amazon y el blog de operaciones y migraciones AWS en la nube, respectivamente.

Para obtener más información sobre CloudWatch Application Signals, consulte Habilitar Amazon CloudWatch Application Insights en la Guía del CloudWatch usuario de Amazon.

Widget de etiquetas

Este widget muestra todas las etiquetas asociadas a la aplicación. Puede utilizar este widget para realizar un seguimiento y administrar los metadatos de la aplicación (criticidad, entorno, centro de costos). Para obtener más información, consulte ¿Qué son las etiquetas? en el documento AWS técnico sobre las mejores prácticas para etiquetar AWS los recursos.

AWS Management Console Acceso privado

AWS Management Console El acceso privado es una función de seguridad avanzada para controlar el acceso a. AWS Management Console AWS Management Console El acceso privado es útil cuando se quiere evitar que los usuarios inicien sesión Cuentas de AWS de forma inesperada desde la red. Con esta función, puede limitar el acceso AWS Management Console únicamente a un conjunto específico de datos conocidos Cuentas de AWS cuando el tráfico se origina dentro de su red.

Temas

Consolas Regiones de AWS de servicio compatibles y funciones

AWS Management Console El acceso privado solo admite un subconjunto de regiones y AWS servicios. Las consolas de servicio no admitidas estarán inactivas en la AWS Management Console. Además, es posible que determinadas AWS Management Console funciones estén deshabilitadas al usar el acceso AWS Management Console privado, por ejemplo, la selección de región predeterminada en la configuración unificada.

Se admiten las siguientes regiones y consolas de servicio.

Regiones admitidas

- US East (Ohio)
- Este de EE. UU. (Norte de Virginia)
- Oeste de EE. UU. (Norte de California)
- Oeste de EE. UU. (Oregón)

- Asia-Pacífico (Hyderabad)
- Asia-Pacífico (Bombay)
- Asia-Pacífico (Seúl)
- Asia-Pacífico (Osaka)
- Asia-Pacífico (Singapur)
- Asia-Pacífico (Sídney)
- Asia-Pacífico (Tokio)
- Canadá (centro)
- Europa (Fráncfort)
- Europa (Irlanda)
- Europa (Londres)
- Europa (París)
- Europa (Estocolmo)
- América del Sur (São Paulo)
- África (Ciudad del Cabo)
- Asia-Pacífico (Hong Kong)
- Asia-Pacífico (Yakarta)
- Asia-Pacífico (Melbourne)
- Oeste de Canadá (Calgary)
- Europa (Milán)
- Europa (España)
- Europa (Zúrich)
- Medio Oriente (Baréin)
- Medio Oriente (EAU)
- Israel (Tel Aviv)

Consolas de servicio admitidas

- Amazon API Gateway
- AWS App Mesh

- AWS Application Migration Service
- Amazon Athena
- AWS Auto Scaling
- AWS Billing Conductor
- AWS Certificate Manager
- AWS Cloud Map
- Amazon CloudFront
- Amazon CloudWatch
- AWS CodeArtifact
- AWS CodeBuild
- Amazon CodeGuru
- Amazon Comprehend
- Amazon Comprehend Medical
- AWS Compute Optimizer
- AWS Console Home
- AWS Database Migration Service
- AWS DeepRacer
- Amazon DocumentDB
- Amazon DynamoDB
- Amazon EC2
- Amazon EC2 Global View
- Generador de Imágenes de EC2
- Conexión de la instancia de Amazon EC2
- Amazon Elastic Container Registry
- Amazon Elastic Container Service
- AWS Elastic Disaster Recovery
- Amazon Elastic File System
- Amazon Elastic Kubernetes Service
- Amazon ElastiCache

- Amazon EMR
- Amazon EventBridge
- Amazon GameLift
- AWS Global Accelerator
- AWS Glue DataBrew
- AWS Ground Station
- Amazon GuardDuty
- AWS Identity and Access Management
- AWS Identity and Access Management Access Analyzer
- Amazon Inspector
- Amazon Kendra
- AWS Key Management Service
- Amazon Kinesis
- Amazon Managed Service para Apache Flink
- Amazon Data Firehose
- Amazon Kinesis Video Streams
- AWS Lambda
- Amazon Lex
- AWS License Manager
- Amazon Managed Grafana
- Transmisión gestionadada de Amazon para Apache Kafka
- Flujos de trabajo administrados por Amazon Managed Workflows for Apache Airflow (MWAA)
- Recomendaciones de estrategias de AWS Migration Hub
- Amazon MQ
- Analizador de acceso a la red
- AWS Network Manager
- OpenSearch Servicio Amazon
- AWS Organizations
- Amazon S3 en Outposts
- Amazon SageMaker Runtime

- Datos SageMaker sintéticos de Amazon
- AWS Secrets Manager
- Service Quotas
- AWS Signer
- Amazon Simple Email Service
- Amazon Simple Queue Service
- Amazon Simple Storage Service (Amazon S3)
- AWS SQL Workbench
- AWS Step Functions
- AWS Support
- AWS Systems Manager
- AWS Transfer Family
- Configuración unificada
- IP Address Manager (IPAM) de Amazon VPC

Descripción general de los controles de seguridad de acceso AWS Management Console privado

Restricciones de cuentas en la AWS Management Console desde su red

AWS Management Console El acceso privado resulta útil en situaciones en las que se desea limitar el acceso AWS Management Console desde la red únicamente a un conjunto específico de personas conocidas Cuentas de AWS en la organización. De este modo, puede evitar que los usuarios inicien sesión en Cuentas de AWS inesperadas desde su red. Puede implementar estos controles mediante la política de puntos de conexión de VPC de la AWS Management Console . Para obtener más información, consulte Implementación de políticas de control de servicio y políticas de punto de conexión de VPC.

Conectividad desde su red a Internet

La conectividad a Internet de la red sigue siendo necesaria para acceder a los activos utilizados por la red AWS Management Console, como el contenido estático (CSSJavaScript, imágenes) y todos los que Servicios de AWS no estén habilitados por ella AWS PrivateLink. Para obtener una

lista de los dominios de nivel superior que utiliza AWS Management Console, consulteResolución de problemas.

> **Note**
>
> Actualmente, AWS Management Console Private Access no admite puntos de conexión como `status.aws.amazon.comhealth.aws.amazon.com`, y. `docs.aws.amazon.com` Deberá enrutar estos dominios a la Internet pública.

Puntos de conexión de VPC y configuración de DNS necesarios

AWS Management Console El acceso privado requiere los siguientes dos puntos de enlace de VPC por región. Reemplace *`región`* por su propia información.

1. com.amazonaws. *`region .console`* para AWS Management Console
2. com.amazonaws. *`región en la`* que iniciar sesión AWS Sign-In

> **Note**
>
> Proporcione siempre conexión de infraestructura y red a la región Este de EE. UU. (Norte de Virginia) (us-east-1), independientemente de las otras regiones que utilice con la AWS Management Console. Se puede utilizar AWS Transit Gateway para configurar la conectividad entre Este de EE. UU. (Norte de Virginia) y cualquier otra región. Para obtener más información, consulte Introducción a las puertas de enlace de tránsito en la Guía de puertas de enlace de tránsito de Amazon VPC. También puede utilizar el emparejamiento de Amazon VPC. Para obtener más información, consulte ¿Qué es una interconexión con VPC? en la Guía de interconexión de Amazon VPC. Para comparar estas opciones, consulte Opciones de conectividad de Amazon VPC a Amazon VPC en el documento técnico de opciones de conectividad de Amazon Virtual Private Cloud.

DNSconfiguración para y AWS Management ConsoleAWS Sign-In

Para dirigir el tráfico de la red a los puntos de conexión de VPC respectivos, configure los registros de DNS de la red desde los que accederán los usuarios a la AWS Management Console. Estos

registros de DNS dirigirán el tráfico del navegador de los usuarios hacia los puntos de conexión de VPC que ha creado.

Puede crear una única zona alojada. Sin embargo, los puntos de conexión como `health.aws.amazon.com` y `docs.aws.amazon.com` no serán accesibles porque no tienen puntos de conexión de VPC. Deberá enrutar estos dominios a la Internet pública. Le recomendamos que cree dos zonas alojadas privadas por región, una para `signin.aws.amazon.com` y otra para `console.aws.amazon.com` con los siguientes registros de CNAME:

- Registros de CNAME regionales (en todas las regiones)
- region.signin.aws.amazon.com apunta al punto final de la VPC en la zona de inicio de sesión AWS Sign-In DNS
- region.console.aws.amazon.com apunta al punto final de la VPC en la zona de la AWS Management Console consola DNS
- Registros de CNAME sin región solo para la región Este de EE. UU. (Norte de Virginia). Siempre hay que configurar la región Este de EE. UU. (Norte de Virginia).
  - signin.aws.amazon.com apunta a un punto final de AWS Sign-In VPC en EE. UU. Este (Norte de Virginia) (us-east-1)
  - console.aws.amazon.com apunta a un punto final de AWS Management Console VPC en EE. UU. Este (Norte de Virginia) (us-east-1)

Para obtener instrucciones sobre cómo crear un registro de CNAME, consulte Working with records (Uso de registros) en la Guía para desarrolladores de Amazon Route 53.

Algunas AWS consolas, incluida Amazon S3, utilizan patrones diferentes para sus DNS nombres. A continuación se muestran dos ejemplos:

- support.console.aws.amazon.com
- s3.console.aws.amazon.com

Para poder dirigir este tráfico a su punto final de AWS Management Console VPC, debe añadir esos nombres de forma individual. Le recomendamos que configure el enrutamiento para todos los puntos de conexión para disfrutar de una experiencia totalmente privada. Sin embargo, esto no es obligatorio para usar el acceso AWS Management Console privado.

Los siguientes `json` archivos contienen la lista completa de Servicio de AWS terminales y terminales de consola que se deben configurar por región. Utilice el campo `PrivateIpv4DnsNames` situado debajo del punto de conexión de `com.amazonaws.region.console` para los nombres de DNS.

- https://configuration.private-access.console.amazonaws.com/us-east-1.config.json
- https://configuration.private-access.console.amazonaws.com/us-east-2.config.json
- https://configuration.private-access.console.amazonaws.com/us-west-2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-northeast-1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-northeast-2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-southeast-1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-southeast-2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-south-1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-south-2.config.json
- https://configuration.private-access.console.amazonaws.com/ca-central-1.config.json
- https://configuration.private-access.console.amazonaws.com/eu-west-1.config.json
- https://configuration.private-access.console.amazonaws.com/eu-west-2.config.json
- https://configuration.private-access.console.amazonaws.com/il-central-1.config.json

> **Note**
>
> Esta lista se actualiza cada mes a medida que añadimos puntos de conexión adicionales al ámbito de AWS Management Console Private Access. Para mantener actualizadas sus zonas alojadas privadas, descargue periódicamente la lista de archivos anterior.

Si usa Route 53 para configurar su DNS, vaya a https://console.aws.amazon.com/route53/v2/hostedzones# para verificar la configuración de DNS. Para cada zona alojada privada de Route 53, compruebe que estén presentes los siguientes conjuntos de registros.

- console.aws.amazon.com
- signin.aws.amazon.com
- region.console.aws.amazon.com
- region.signin.aws.amazon.com
- support.console.aws.amazon.com

- global.console.aws.amazon.com
- Registros adicionales presentes en los archivos JSON enumerados anteriormente

Terminales de VPC y configuración de servicios DNSAWS

Las AWS Management Console llamadas se Servicios de AWS realizan mediante una combinación de solicitudes directas del navegador y solicitudes enviadas por proxy desde servidores web. Para dirigir este tráfico a su punto de enlace de AWS Management Console VPC, debe agregar el punto de enlace de VPC y configurarlo DNS para cada servicio dependiente. AWS

En los siguientes json archivos se enumeran los archivos AWS PrivateLink compatibles Servicios de AWS que están disponibles para su uso. Si un servicio no se integra con AWS PrivateLink, no se incluye en estos archivos.

- https://configuration.private-access.console.amazonaws.com/us-east-1.config.json
- https://configuration.private-access.console.amazonaws.com/us-east-2.config.json
- https://configuration.private-access.console.amazonaws.com/us-west-2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-northeast-1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-northeast-2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-southeast-1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-southeast-2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-south-1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-south-2.config.json
- https://configuration.private-access.console.amazonaws.com/ca-central-1.config.json
- https://configuration.private-access.console.amazonaws.com/eu-west-1.config.json
- https://configuration.private-access.console.amazonaws.com/eu-west-2.config.json
- https://configuration.private-access.console.amazonaws.com/il-central-1.config.json

Use el campo `ServiceName` del punto de conexión de VPC del servicio correspondiente para añadirlo a su VPC.

> **Note**
>
> Actualizamos esta lista todos los meses a medida que añadimos la compatibilidad con el acceso AWS Management Console privado a más consolas de servicio. Para mantenerse al

día, descargue periódicamente la lista de archivos anterior y actualice los puntos de conexión de VPC.

Implementación de políticas de control de servicio y políticas de punto de conexión de VPC

Puede usar políticas de control de servicios (SCP) y políticas de punto final de VPC AWS Management Console para el acceso privado a fin de limitar el conjunto de cuentas que pueden usar AWS Management Console la VPC y sus redes locales conectadas.

Uso del acceso AWS Management Console privado con políticas de control de servicios AWS Organizations

Si su AWS organización utiliza una política de control de servicios (SCP) que permite servicios específicos, debe `signin:*` añadir más acciones permitidas. Este permiso es necesario porque al iniciar sesión a AWS Management Console través de un punto final de VPC de acceso privado se produce una autorización de IAM que el SCP bloquea sin el permiso. A modo de ejemplo, la siguiente política de control de servicios permite utilizar Amazon EC2 y sus CloudWatch servicios en la organización, incluso cuando se accede a ellos mediante un punto final de acceso AWS Management Console privado.

```
{
  "Effect": "Allow",
  "Action": [
    "signin:*",
    "ec2:*",
    "cloudwatch:*",
    ... Other services allowed
  },
  "Resource": "*"
}
```

Para obtener más información acerca de las SCP, consulte Políticas de control de servicios (SCP) en la Guía del usuario de AWS Organizations .

Permita AWS Management Console su uso únicamente para las cuentas y organizaciones esperadas (identidades de confianza)

AWS Management Console y AWS Sign-In admiten una política de puntos finales de VPC que controle específicamente la identidad de la cuenta en la que se ha iniciado sesión.

A diferencia de otras políticas de punto de conexión de VPC, la política se evalúa antes de la autenticación. Como resultado, controla específicamente el inicio de sesión y el uso únicamente de la sesión autenticada, y no las acciones específicas del AWS servicio que lleve a cabo la sesión. Por ejemplo, cuando la sesión accede a una consola de AWS servicio, como la consola de Amazon EC2, estas políticas de punto final de VPC no se evaluarán en función de las acciones de Amazon EC2 que se tomen para mostrar esa página. En su lugar, puede utilizar las políticas de IAM asociadas al director de IAM que ha iniciado sesión para controlar sus permisos para realizar acciones. AWS

> **Note**
>
> Las políticas de puntos finales de VPC y los puntos finales de AWS Management Console SignIn VPC solo admiten un subconjunto limitado de formulaciones de políticas. Cada `Principal` y `Resource` se debe establecer a `*` y la `Action` debe ser `*` o `signin:*`. El acceso a los puntos de conexión de VPC se controla mediante las claves de condición `aws:PrincipalOrgId` y `aws:PrincipalAccount`.

Se recomiendan las siguientes políticas para los puntos finales de la consola y de la SignIn VPC.

Esta política de punto final de VPC permite iniciar sesión Cuentas de AWS en la AWS organización especificada y bloquea el inicio de sesión en cualquier otra cuenta.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalOrgId": "o-xxxxxxxxxxx"
```

```
        }
      }
    }
  ]
}
```

Esta política de puntos finales de VPC limita el inicio de sesión a una lista de cuentas específicas Cuentas de AWS y bloquea el inicio de sesión en cualquier otra cuenta.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalAccount": [ "111122223333", "222233334444" ]
        }
      }
    }
  ]
}
```

Las políticas que limitan Cuentas de AWS una organización en los puntos finales de la VPC AWS Management Console y de inicio de sesión se evalúan en el momento del inicio de sesión y se vuelven a evaluar periódicamente para las sesiones existentes.

Implementación de políticas basadas en identidad y otros tipos de políticas

AWS Para gestionar el acceso, debe crear políticas y adjuntarlas a las identidades de IAM (usuarios, grupos de usuarios o funciones) o a los recursos. AWS En esta página, se describe cómo funcionan las políticas cuando se utilizan junto con AWS Management Console Private Access.

Claves de contexto de condición AWS global compatibles

AWS Management Console El acceso privado no admite `aws:SourceVpce` ninguna clave de contexto de condición `aws:VpcSourceIp` AWS global. En su lugar, puede utilizar la condición de IAM `aws:SourceVpc` en sus políticas cuando utilice AWS Management Console Private Access.

Cómo funciona AWS Management Console Private Access con AWS: SourceVpc

En esta sección se describen las distintas rutas de red a las que AWS Management Console pueden dirigirse las solicitudes generadas por usted Servicios de AWS. En general, las consolas de AWS servicio se implementan con una combinación de solicitudes directas del navegador y solicitudes enviadas por proxy desde los servidores AWS Management Console web. Servicios de AWS Estas implementaciones están sujetas a cambios sin previo aviso. Si sus requisitos de seguridad incluyen el acceso al Servicios de AWS uso de puntos de enlace de VPC, le recomendamos que configure los puntos de enlace de VPC para todos los servicios que desee utilizar desde la VPC, ya sea directamente o mediante acceso privado. AWS Management Console Además, debe utilizar la condición de `aws:SourceVpc` IAM en sus políticas en lugar de `aws:SourceVpce` valores específicos con la función de acceso privado. AWS Management Console En esta sección, se proporcionan detalles sobre cómo funcionan las diferentes rutas de red.

Una vez que un usuario inicia sesión en AWS Management Console, realiza las solicitudes Servicios de AWS mediante una combinación de solicitudes directas del navegador y solicitudes que los servidores AWS Management Console web envían mediante proxy a AWS los servidores. Por ejemplo, las solicitudes de datos CloudWatch gráficos se realizan directamente desde el navegador. Mientras que algunas solicitudes de la consola de AWS servicio, como Amazon S3, se envían mediante proxy desde el servidor web a Amazon S3.

En el caso de las solicitudes directas desde el navegador, el uso del acceso AWS Management Console privado no supone ningún cambio. Como antes, la solicitud llega al servicio a través de cualquier ruta de red para la que la VPC esté configurada para llegar a monitoring.region.amazonaws.com. Si la VPC está configurada con un punto de enlace de VPC paracom.amazonaws.region.monitoring, la solicitud llegará a través de CloudWatch ese punto de enlace de VPC. CloudWatch Si no hay ningún punto final de la VPC CloudWatch, la solicitud llegará a su punto final público, CloudWatch a través de una puerta de enlace de Internet en la VPC. Las solicitudes que lleguen a CloudWatch través del punto final de la CloudWatch VPC tendrán las condiciones de IAM `aws:SourceVpc` y se `aws:SourceVpce` establecerán en sus valores respectivos. Las que accedan CloudWatch a través de su punto final público deberán

`aws:SourceIp` configurar la dirección IP de origen de la solicitud. Para obtener más información sobre estas claves de condición de IAM, consulte Claves de condición global en la Guía del usuario de IAM.

En el caso de las solicitudes que el servidor AWS Management Console web envía mediante proxy, como la solicitud que hace la consola Amazon S3 para incluir sus buckets cuando visita la consola Amazon S3, la ruta de red es diferente. Estas solicitudes no se inician desde la VPC y, por lo tanto, no utilizan el punto de conexión de VPC que es posible que haya configurado en la VPC para ese servicio. Incluso si, en este caso, tiene un punto de conexión de VPC para Amazon S3, la solicitud de su sesión a Amazon S3 para enumerar los buckets no utiliza el punto de conexión de VPC de Amazon S3. Sin embargo, cuando utilice el acceso AWS Management Console privado con los servicios compatibles, estas solicitudes (por ejemplo, a Amazon S3) incluirán la clave de `aws:SourceVpc` condición en el contexto de la solicitud. La clave de `aws:SourceVpc` condición se establecerá en el ID de VPC en el que se implementan los puntos finales de acceso AWS Management Console privado para el inicio de sesión y la consola. Por lo tanto, si utiliza restricciones `aws:SourceVpc` en sus políticas basadas en identidad, debe añadir el ID de esta VPC que aloja los puntos de conexión de consola y de inicio de sesión de AWS Management Console Private Access. La condición `aws:SourceVpce` se establecerá en los respectivos ID de punto de conexión de VPC de la consola o el inicio de sesión.

> **Note**
>
> Si los usuarios requieren acceso a las consolas de servicio que no son compatibles con AWS Management Console Private Access, debe incluir una lista de las direcciones de red pública esperadas (como el rango de redes en las instalaciones) mediante la clave de condición `aws:SourceIP` en las políticas basadas en identidades de los usuarios.

Cómo se reflejan las diferentes rutas de red en CloudTrail

Las diferentes rutas de red utilizadas por las solicitudes generadas por AWS Management Console usted se reflejan en su historial de CloudTrail eventos.

En el caso de las solicitudes directas desde el navegador, el uso del acceso AWS Management Console privado no cambia nada. CloudTrail los eventos incluirán detalles sobre la conexión, como el ID del punto final de la VPC que se utilizó para realizar la llamada a la API del servicio.

En el caso de las solicitudes enviadas por proxy por el servidor AWS Management Console web, CloudTrail los eventos no incluirán ningún detalle relacionado con la VPC. Sin embargo, las

solicitudes iniciales necesarias para AWS Sign-In establecer la sesión del navegador, como el tipo de `AwsConsoleSignIn` evento, incluirán el ID del punto final de la AWS Sign-In VPC en los detalles del evento.

Prueba con AWS Management Console Private Access

En esta sección se describe cómo configurar y probar el acceso AWS Management Console privado en una cuenta nueva.

AWS Management Console El acceso privado es una función de seguridad avanzada y requiere conocimientos previos sobre las redes y la configuración de las VPC. En este tema, se describe cómo puede probar AWS Management Console Private Access sin una infraestructura a gran escala.

Temas

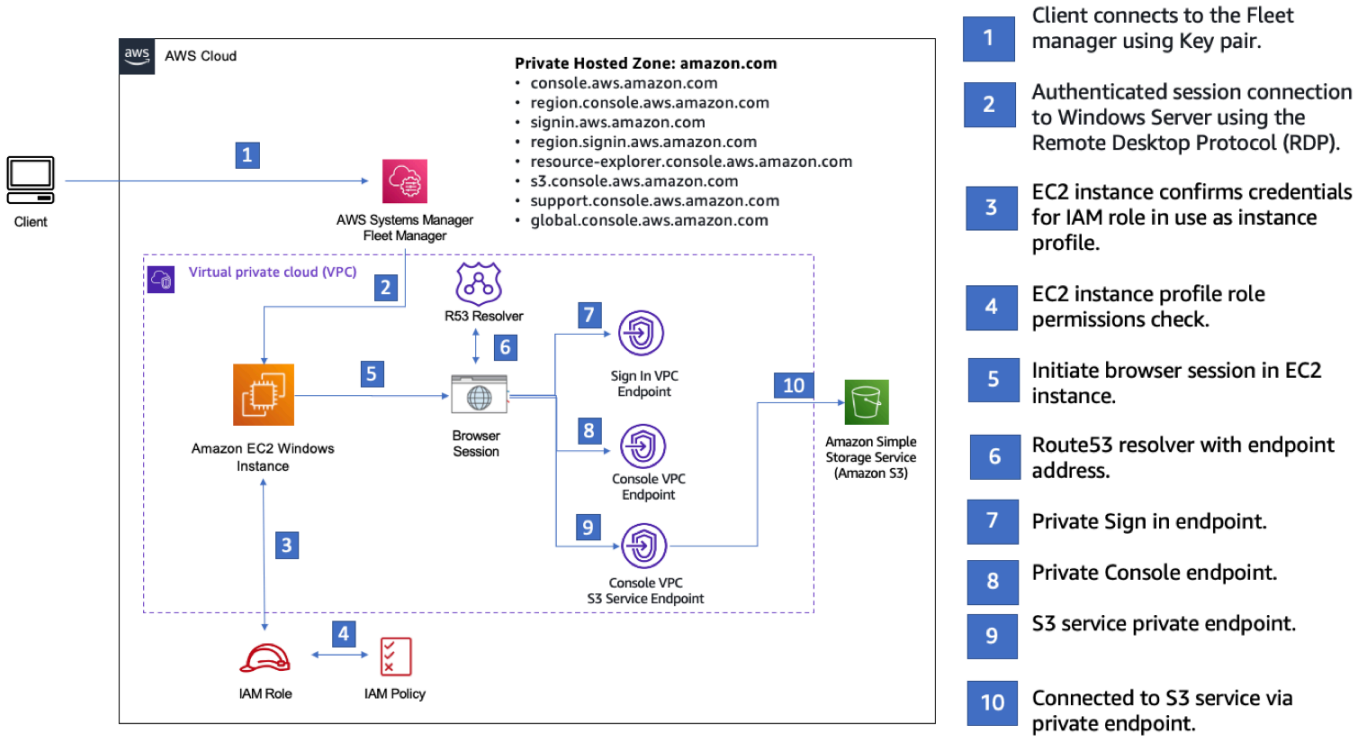
- Configuración de prueba con Amazon EC2
- Configuración de prueba con Amazon WorkSpaces
- Pruebe la configuración de la VPC con políticas de IAM

Configuración de prueba con Amazon EC2

Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad de computación escalable en la nube de Amazon Web Services. Puede usar Amazon EC2 para lanzar tantos servidores virtuales como necesite, configurar la seguridad y las redes, y administrar el almacenamiento. En esta configuración, puede utilizar Fleet Manager, una capacidad de AWS Systems Manager, para conectarse a sus instancias de Windows de Amazon EC2 mediante el protocolo de escritorio remoto (RDP).

Esta guía muestra un entorno de prueba para configurar y experimentar una conexión de acceso AWS Management Console privado a Amazon Simple Storage Service desde una instancia de Amazon EC2. Este tutorial se utiliza AWS CloudFormation para crear y configurar la configuración de red que utilizará Amazon EC2 para visualizar esta función.

El siguiente diagrama describe el flujo de trabajo para usar Amazon EC2 para acceder a una configuración de AWS Management Console Private Access. Muestra cómo se conecta un usuario a Amazon S3 mediante un punto de conexión privado.



Copie la siguiente AWS CloudFormation plantilla y guárdela en un archivo que utilizará en el paso tres del procedimiento Para configurar una red.

> **Note**
>
> Esta AWS CloudFormation plantilla utiliza configuraciones que actualmente no se admiten en la región de Israel (Tel Aviv).

AWS Management Console Plantilla Amazon AWS CloudFormation EC2 del entorno de acceso privado

```
Description: |
  AWS Management Console Private Access.
Parameters:
  VpcCIDR:
    Type: String
    Default: 172.16.0.0/16
    Description: CIDR range for VPC
```

```
  Ec2KeyPair:
    Type: AWS::EC2::KeyPair::KeyName
    Description: The EC2 KeyPair to use to connect to the Windows instance

  PublicSubnet1CIDR:
    Type: String
    Default: 172.16.1.0/24
    Description: CIDR range for Public Subnet A

  PublicSubnet2CIDR:
    Type: String
    Default: 172.16.0.0/24
    Description: CIDR range for Public Subnet B

  PublicSubnet3CIDR:
    Type: String
    Default: 172.16.2.0/24
    Description: CIDR range for Public Subnet C

  PrivateSubnet1CIDR:
    Type: String
    Default: 172.16.4.0/24
    Description: CIDR range for Private Subnet A

  PrivateSubnet2CIDR:
    Type: String
    Default: 172.16.5.0/24
    Description: CIDR range for Private Subnet B

  PrivateSubnet3CIDR:
    Type: String
    Default: 172.16.3.0/24
    Description: CIDR range for Private Subnet C

  LatestWindowsAmiId:
    Type: 'AWS::SSM::Parameter::Value<AWS::EC2::Image::Id>'
    Default: '/aws/service/ami-windows-latest/Windows_Server-2022-English-Full-Base'

  InstanceTypeParameter:
    Type: String
    Default: 't2.medium'


Resources:
```

```
#########################
# VPC AND SUBNETS
#########################

  AppVPC:
    Type: 'AWS::EC2::VPC'
    Properties:
      CidrBlock: !Ref VpcCIDR
      InstanceTenancy: default
      EnableDnsSupport: true
      EnableDnsHostnames: true

  PublicSubnetA:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PublicSubnet1CIDR
      MapPublicIpOnLaunch: true
      AvailabilityZone:
        Fn::Select:
          - 0
          - Fn::GetAZs: ""

  PublicSubnetB:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PublicSubnet2CIDR
      MapPublicIpOnLaunch: true
      AvailabilityZone:
        Fn::Select:
          - 1
          - Fn::GetAZs: ""

  PublicSubnetC:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PublicSubnet3CIDR
      MapPublicIpOnLaunch: true
      AvailabilityZone:
        Fn::Select:
          - 2
```

```
        - Fn::GetAZs: ""

  PrivateSubnetA:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PrivateSubnet1CIDR
      AvailabilityZone:
        Fn::Select:
          - 0
          - Fn::GetAZs: ""

  PrivateSubnetB:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PrivateSubnet2CIDR
      AvailabilityZone:
        Fn::Select:
          - 1
          - Fn::GetAZs: ""

  PrivateSubnetC:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PrivateSubnet3CIDR
      AvailabilityZone:
        Fn::Select:
          - 2
          - Fn::GetAZs: ""

  InternetGateway:
    Type: AWS::EC2::InternetGateway

  InternetGatewayAttachment:
    Type: AWS::EC2::VPCGatewayAttachment
    Properties:
      InternetGatewayId: !Ref InternetGateway
      VpcId: !Ref AppVPC

  NatGatewayEIP:
    Type: AWS::EC2::EIP
    DependsOn: InternetGatewayAttachment
```

```
  NatGateway:
    Type: AWS::EC2::NatGateway
    Properties:
      AllocationId: !GetAtt NatGatewayEIP.AllocationId
      SubnetId: !Ref PublicSubnetA

########################
# Route Tables
########################

  PrivateRouteTable:
    Type: 'AWS::EC2::RouteTable'
    Properties:
      VpcId: !Ref AppVPC

  DefaultPrivateRoute:
    Type: AWS::EC2::Route
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      NatGatewayId: !Ref NatGateway

  PrivateSubnetRouteTableAssociation1:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      SubnetId: !Ref PrivateSubnetA

  PrivateSubnetRouteTableAssociation2:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      SubnetId: !Ref PrivateSubnetB

  PrivateSubnetRouteTableAssociation3:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      SubnetId: !Ref PrivateSubnetC

  PublicRouteTable:
    Type: AWS::EC2::RouteTable
    Properties:
```

```
      VpcId: !Ref AppVPC

  DefaultPublicRoute:
    Type: AWS::EC2::Route
    DependsOn: InternetGatewayAttachment
    Properties:
      RouteTableId: !Ref PublicRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      GatewayId: !Ref InternetGateway

  PublicSubnetARouteTableAssociation1:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref PublicRouteTable
      SubnetId: !Ref PublicSubnetA

  PublicSubnetBRouteTableAssociation2:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref PublicRouteTable
      SubnetId: !Ref PublicSubnetB

  PublicSubnetBRouteTableAssociation3:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref PublicRouteTable
      SubnetId: !Ref PublicSubnetC


##########################
# SECURITY GROUPS
##########################

  VPCEndpointSecurityGroup:
    Type: 'AWS::EC2::SecurityGroup'
    Properties:
      GroupDescription: Allow TLS for VPC Endpoint
      VpcId: !Ref AppVPC
      SecurityGroupIngress:
        - IpProtocol: tcp
          FromPort: 443
          ToPort: 443
          CidrIp: !GetAtt AppVPC.CidrBlock
```

```
  EC2SecurityGroup:
    Type: 'AWS::EC2::SecurityGroup'
    Properties:
      GroupDescription: Default EC2 Instance SG
      VpcId: !Ref AppVPC

#########################
# VPC ENDPOINTS
#########################

  VPCEndpointGatewayS3:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.s3'
      VpcEndpointType: Gateway
      VpcId: !Ref AppVPC
      RouteTableIds:
        - !Ref PrivateRouteTable

  VPCEndpointInterfaceSSM:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.ssm'
      VpcId: !Ref AppVPC

  VPCEndpointInterfaceEc2messages:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
        - !Ref PrivateSubnetC
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.ec2messages'
```

```
      VpcId: !Ref AppVPC

  VPCEndpointInterfaceSsmmessages:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
        - !Ref PrivateSubnetC
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.ssmmessages'
      VpcId: !Ref AppVPC

  VPCEndpointInterfaceSignin:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
        - !Ref PrivateSubnetC
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.signin'
      VpcId: !Ref AppVPC

  VPCEndpointInterfaceConsole:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
        - !Ref PrivateSubnetC
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.console'
      VpcId: !Ref AppVPC
```

```
#########################
# ROUTE53 RESOURCES
#########################

  ConsoleHostedZone:
    Type: "AWS::Route53::HostedZone"
    Properties:
      HostedZoneConfig:
        Comment: 'Console VPC Endpoint Hosted Zone'
      Name: 'console.aws.amazon.com'
      VPCs:
        -
          VPCId: !Ref AppVPC
          VPCRegion: !Ref "AWS::Region"

  ConsoleRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 'console.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  GlobalConsoleRecord:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 'global.console.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  ConsoleS3ProxyRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 's3.console.aws.amazon.com'
```

```
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  ConsoleSupportProxyRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: "support.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  ExplorerProxyRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: "resource-explorer.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  ConsoleRecordRegional:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: !Sub "${AWS::Region}.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  SigninHostedZone:
```

```
    Type: "AWS::Route53::HostedZone"
    Properties:
      HostedZoneConfig:
        Comment: 'Signin VPC Endpoint Hosted Zone'
      Name: 'signin.aws.amazon.com'
      VPCs:
        -
          VPCId: !Ref AppVPC
          VPCRegion: !Ref "AWS::Region"

  SigninRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'SigninHostedZone'
      Name: 'signin.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
      Type: A

  SigninRecordRegional:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'SigninHostedZone'
      Name: !Sub "${AWS::Region}.signin.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
      Type: A

#########################
# EC2 INSTANCE
#########################

  Ec2InstanceRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
```

```
        -
          Effect: Allow
          Principal:
            Service:
              - ec2.amazonaws.com
          Action:
            - sts:AssumeRole
    Path: /
    ManagedPolicyArns:
      - arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore

Ec2InstanceProfile:
  Type: AWS::IAM::InstanceProfile
  Properties:
    Path: /
    Roles:
     - !Ref Ec2InstanceRole

EC2WinInstance:
  Type: 'AWS::EC2::Instance'
  Properties:
    ImageId: !Ref LatestWindowsAmiId
    IamInstanceProfile: !Ref Ec2InstanceProfile
    KeyName: !Ref Ec2KeyPair
    InstanceType:
      Ref: InstanceTypeParameter
    SubnetId: !Ref PrivateSubnetA
    SecurityGroupIds:
      - Ref: EC2SecurityGroup
    BlockDeviceMappings:
      - DeviceName: /dev/sda1
        Ebs:
          VolumeSize: 50
    Tags:
    - Key: "Name"
      Value: "Console VPCE test instance"
```

Para configurar una red

1. Inicie sesión en la cuenta de administración de su organización y abra la consola de AWS CloudFormation.
2. Seleccione Crear pila.

3. Elija With new resources (standard) (Con nuevos recursos [estándar]). Cargue el archivo de AWS CloudFormation plantilla que creó anteriormente y seleccione Siguiente.
4. Introduzca un nombre para la pila (por ejemplo, **`PrivateConsoleNetworkForS3`**) y, a continuación, seleccione Siguiente.
5. Para VPC y subredes, introduzca los rangos de CIDR de IP que prefiera o use los valores predeterminados proporcionados. Si utilizas los valores predeterminados, comprueba que no se superpongan con los recursos de VPC existentes en tu empresa. Cuenta de AWS
6. Para el KeyPair parámetro Ec2, seleccione uno de los pares de claves de Amazon EC2 existentes en su cuenta. Si no tiene un par de claves de Amazon EC2 existente, deberá crear uno antes de continuar con el siguiente paso. Para obtener más información, consulte Creación de un par de claves con Amazon EC2 en la Guía del usuario de Amazon EC2.
7. Seleccione Crear pila.
8. Una vez creada la pila, elija la pestaña Recursos para ver los recursos que se han creado.

Para conectarse con la instancia de Amazon EC2:

1. Inicie sesión en la cuenta de administración de su organización y abra la consola de Amazon EC2.
2. En el panel de navegación, seleccione Instancias.
3. En la página Instancias, seleccione la instancia de prueba VPCE de consola creada por la plantilla. AWS CloudFormation A continuación, elija Conectar.

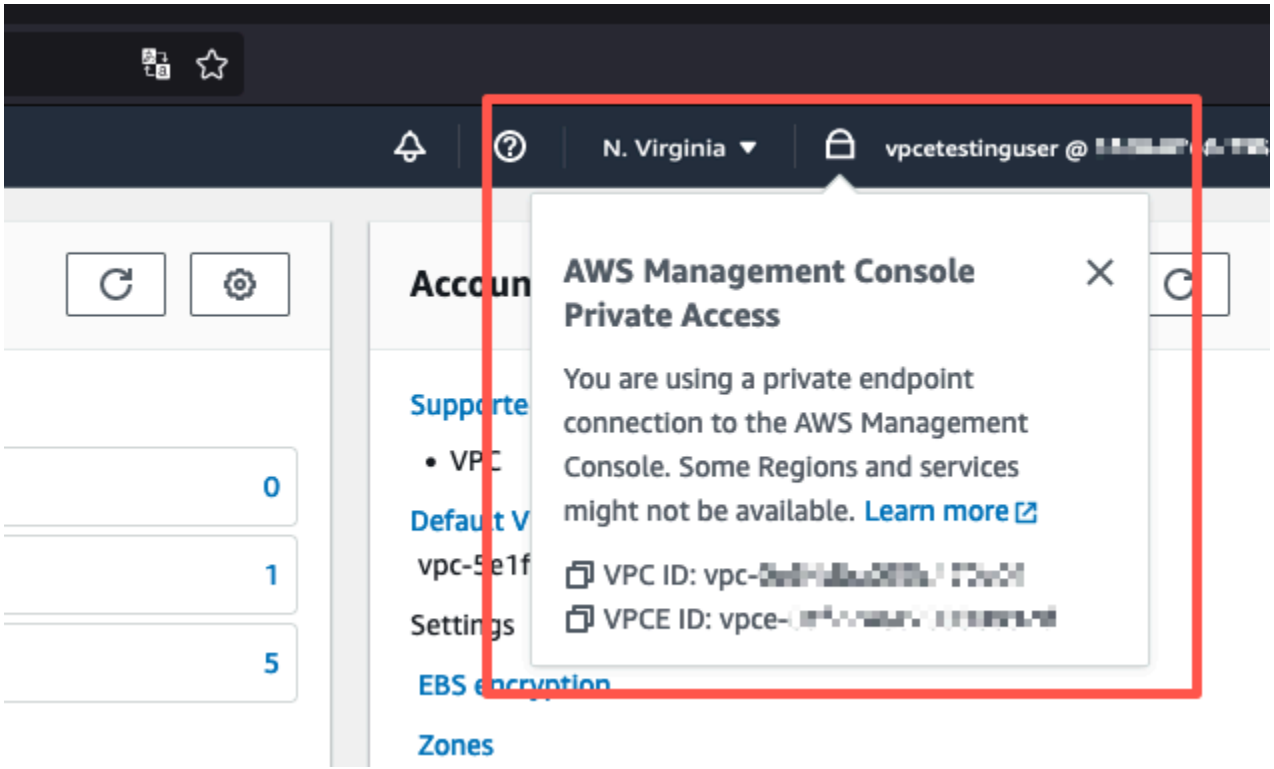
> **Note**
>
> En este ejemplo, se utiliza Fleet Manager, una capacidad de AWS Systems Manager Explorer, para conectarse a su servidor Windows. Puede que tarde unos minutos en iniciar la conexión.

4. En la página Conectarse a la instancia, seleccione Cliente de RDP y, a continuación, Conectarse mediante Fleet Manager.
5. Elija Escritorio remoto de Fleet Manager.
6. Para obtener la contraseña administrativa de la instancia de Amazon EC2 y acceder al escritorio de Windows mediante la interfaz web, utilice la clave privada asociada al par de claves de Amazon EC2 que utilizó al AWS CloudFormation crear la plantilla.

7. Desde la instancia Amazon EC2 de Windows, abra el AWS Management Console en el navegador.
8. Tras iniciar sesión con sus AWS credenciales, abra la consola de Amazon S3 y compruebe que está conectado mediante acceso AWS Management Console privado.

Para probar la configuración del acceso AWS Management Console privado

1. Inicie sesión en la cuenta de administración de su organización y abra la consola de Amazon S3.
2. Elija el icono del candado privado en la barra de navegación para ver el punto de conexión de VPC en uso. La siguiente captura de pantalla muestra la ubicación del icono del candado y la información de la VPC.



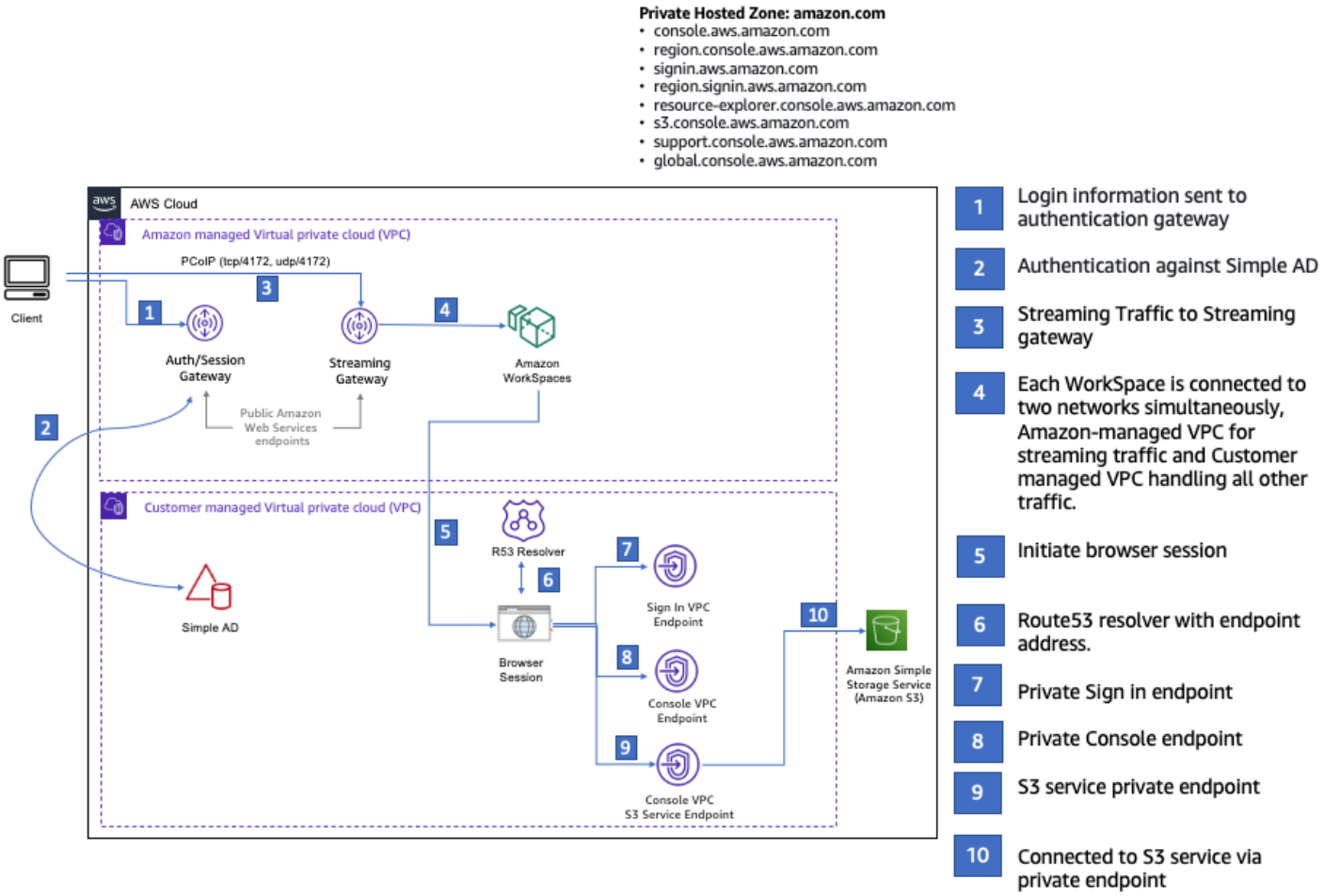
Configuración de prueba con Amazon WorkSpaces

Amazon WorkSpaces le permite aprovisionar escritorios Windows, Amazon Linux o Ubuntu Linux virtuales basados en la nube para sus usuarios, lo que se conoce como WorkSpaces. Puede agregar o eliminar rápidamente a los usuarios en función de las necesidades. Los usuarios tienen acceso a los escritorios virtuales desde diversos dispositivos o navegadores web. Para obtener más información WorkSpaces, consulta la Guía de WorkSpaces administración de Amazon.

El ejemplo de esta sección describe un entorno de prueba en el que un entorno de usuario utiliza un navegador web que se ejecuta en un WorkSpace para iniciar sesión en AWS Management Console Private Access. A continuación, el usuario visita la consola de Amazon Simple Storage Service. WorkSpace El objetivo es simular la experiencia de un usuario corporativo con un portátil en una red conectada a VPC, accediendo a ella AWS Management Console desde su navegador.

Este tutorial se utiliza AWS CloudFormation para crear y configurar la configuración de la red y un Active Directory simple para su uso, WorkSpaces junto con instrucciones paso a paso para configurar un WorkSpace mediante. AWS Management Console

El siguiente diagrama describe el flujo de trabajo que se utiliza WorkSpace para probar una configuración de acceso AWS Management Console privado. Muestra la relación entre un cliente WorkSpace, una VPC gestionada por Amazon y una VPC gestionada por el cliente.



Copie la siguiente AWS CloudFormation plantilla y guárdela en un archivo que utilizará en el paso 3 del procedimiento para configurar una red.

AWS Management ConsoleAWS CloudFormation Plantilla de entorno de acceso privado

```
Description: |
  AWS Management Console Private Access.
Parameters:

  VpcCIDR:
    Type: String
    Default: 172.16.0.0/16
    Description: CIDR range for VPC

  PublicSubnet1CIDR:
    Type: String
    Default: 172.16.1.0/24
    Description: CIDR range for Public Subnet A

  PublicSubnet2CIDR:
    Type: String
    Default: 172.16.0.0/24
    Description: CIDR range for Public Subnet B

  PrivateSubnet1CIDR:
    Type: String
    Default: 172.16.4.0/24
    Description: CIDR range for Private Subnet A

  PrivateSubnet2CIDR:
    Type: String
    Default: 172.16.5.0/24
    Description: CIDR range for Private Subnet B

# Amazon WorkSpaces is available in a subset of the Availability Zones for each
 supported Region.
# https://docs.aws.amazon.com/workspaces/latest/adminguide/azs-workspaces.html
Mappings:
  RegionMap:
    us-east-1:
      az1: use1-az2
      az2: use1-az4
      az3: use1-az6
    us-west-2:
      az1: usw2-az1
      az2: usw2-az2
      az3: usw2-az3
```

```
    ap-south-1:
      az1: aps1-az1
      az2: aps1-az2
      az3: aps1-az3
    ap-northeast-2:
      az1: apne2-az1
      az2: apne2-az3
    ap-southeast-1:
      az1: apse1-az1
      az2: apse1-az2
    ap-southeast-2:
      az1: apse2-az1
      az2: apse2-az3
    ap-northeast-1:
      az1: apne1-az1
      az2: apne1-az4
    ca-central-1:
      az1: cac1-az1
      az2: cac1-az2
    eu-central-1:
      az1: euc1-az2
      az2: euc1-az3
    eu-west-1:
      az1: euw1-az1
      az2: euw1-az2
    eu-west-2:
      az1: euw2-az2
      az2: euw2-az3
    sa-east-1:
      az1: sae1-az1
      az2: sae1-az3

Resources:

  iamLambdaExecutionRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service:
              - lambda.amazonaws.com
```

```
            Action:
              - 'sts:AssumeRole'
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole
      Policies:
        - PolicyName: describe-ec2-az
          PolicyDocument:
            Version: "2012-10-17"
            Statement:
              - Effect: Allow
                Action:
                  - 'ec2:DescribeAvailabilityZones'
                Resource: '*'
      MaxSessionDuration: 3600
      Path: /service-role/

  fnZoneIdtoZoneName:
    Type: AWS::Lambda::Function
    Properties:
      Runtime: python3.8
      Handler: index.lambda_handler
      Code:
        ZipFile: |
          import boto3
          import cfnresponse

          def zoneId_to_zoneName(event, context):
              responseData = {}
              ec2 = boto3.client('ec2')
              describe_az = ec2.describe_availability_zones()
              for az in describe_az['AvailabilityZones']:
                  if event['ResourceProperties']['ZoneId'] == az['ZoneId']:
                      responseData['ZoneName'] = az['ZoneName']
                      cfnresponse.send(event, context, cfnresponse.SUCCESS,
responseData, str(az['ZoneId']))

          def no_op(event, context):
              print(event)
              responseData = {}
              cfnresponse.send(event, context, cfnresponse.SUCCESS, responseData,
str(event['RequestId']))

          def lambda_handler(event, context):
              if event['RequestType'] == ('Create' or 'Update'):
```

```
                zoneId_to_zoneName(event, context)
            else:
                no_op(event,context)
      Role: !GetAtt iamLambdaExecutionRole.Arn

  getAZ1:
    Type: "Custom::zone-id-zone-name"
    Properties:
      ServiceToken: !GetAtt fnZoneIdtoZoneName.Arn
      ZoneId: !FindInMap [ RegionMap, !Ref 'AWS::Region', az1 ]
  getAZ2:
    Type: "Custom::zone-id-zone-name"
    Properties:
      ServiceToken: !GetAtt fnZoneIdtoZoneName.Arn
      ZoneId: !FindInMap [ RegionMap, !Ref 'AWS::Region', az2 ]

#########################
# VPC AND SUBNETS
#########################

  AppVPC:
    Type: 'AWS::EC2::VPC'
    Properties:
      CidrBlock: !Ref VpcCIDR
      InstanceTenancy: default
      EnableDnsSupport: true
      EnableDnsHostnames: true

  PublicSubnetA:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PublicSubnet1CIDR
      MapPublicIpOnLaunch: true
      AvailabilityZone: !GetAtt getAZ1.ZoneName

  PublicSubnetB:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PublicSubnet2CIDR
      MapPublicIpOnLaunch: true
      AvailabilityZone: !GetAtt getAZ2.ZoneName
```

```
  PrivateSubnetA:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PrivateSubnet1CIDR
      AvailabilityZone: !GetAtt getAZ1.ZoneName

  PrivateSubnetB:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PrivateSubnet2CIDR
      AvailabilityZone: !GetAtt getAZ2.ZoneName

  InternetGateway:
    Type: AWS::EC2::InternetGateway

  InternetGatewayAttachment:
    Type: AWS::EC2::VPCGatewayAttachment
    Properties:
      InternetGatewayId: !Ref InternetGateway
      VpcId: !Ref AppVPC

  NatGatewayEIP:
    Type: AWS::EC2::EIP
    DependsOn: InternetGatewayAttachment

  NatGateway:
    Type: AWS::EC2::NatGateway
    Properties:
      AllocationId: !GetAtt NatGatewayEIP.AllocationId
      SubnetId: !Ref PublicSubnetA

##########################
# Route Tables
##########################

  PrivateRouteTable:
    Type: 'AWS::EC2::RouteTable'
    Properties:
      VpcId: !Ref AppVPC

  DefaultPrivateRoute:
    Type: AWS::EC2::Route
```

```
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      NatGatewayId: !Ref NatGateway

  PrivateSubnetRouteTableAssociation1:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      SubnetId: !Ref PrivateSubnetA

  PrivateSubnetRouteTableAssociation2:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      SubnetId: !Ref PrivateSubnetB

  PublicRouteTable:
    Type: AWS::EC2::RouteTable
    Properties:
      VpcId: !Ref AppVPC

  DefaultPublicRoute:
    Type: AWS::EC2::Route
    DependsOn: InternetGatewayAttachment
    Properties:
      RouteTableId: !Ref PublicRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      GatewayId: !Ref InternetGateway

  PublicSubnetARouteTableAssociation1:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref PublicRouteTable
      SubnetId: !Ref PublicSubnetA

  PublicSubnetBRouteTableAssociation2:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref PublicRouteTable
      SubnetId: !Ref PublicSubnetB


##########################
```

```
# SECURITY GROUPS
#########################

  VPCEndpointSecurityGroup:
    Type: 'AWS::EC2::SecurityGroup'
    Properties:
      GroupDescription: Allow TLS for VPC Endpoint
      VpcId: !Ref AppVPC
      SecurityGroupIngress:
        - IpProtocol: tcp
          FromPort: 443
          ToPort: 443
          CidrIp: !GetAtt AppVPC.CidrBlock

#########################
# VPC ENDPOINTS
#########################

  VPCEndpointGatewayS3:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.s3'
      VpcEndpointType: Gateway
      VpcId: !Ref AppVPC
      RouteTableIds:
        - !Ref PrivateRouteTable

  VPCEndpointInterfaceSignin:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.signin'
      VpcId: !Ref AppVPC

  VPCEndpointInterfaceConsole:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
```

```
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.console'
      VpcId: !Ref AppVPC

#########################
# ROUTE53 RESOURCES
#########################

  ConsoleHostedZone:
    Type: "AWS::Route53::HostedZone"
    Properties:
      HostedZoneConfig:
        Comment: 'Console VPC Endpoint Hosted Zone'
      Name: 'console.aws.amazon.com'
      VPCs:
        -
          VPCId: !Ref AppVPC
          VPCRegion: !Ref "AWS::Region"

  ConsoleRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 'console.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  GlobalConsoleRecord:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 'global.console.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceConsole.DnsEntries]]]
```

```
       HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
     Type: A

 ConsoleS3ProxyRecordGlobal:
   Type: AWS::Route53::RecordSet
   Properties:
     HostedZoneId: !Ref 'ConsoleHostedZone'
     Name: 's3.console.aws.amazon.com'
     AliasTarget:
       DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
       HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
     Type: A

 ConsoleSupportProxyRecordGlobal:
   Type: AWS::Route53::RecordSet
   Properties:
     HostedZoneId: !Ref 'ConsoleHostedZone'
     Name: "support.console.aws.amazon.com"
     AliasTarget:
       DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
       HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
     Type: A

 ExplorerProxyRecordGlobal:
   Type: AWS::Route53::RecordSet
   Properties:
     HostedZoneId: !Ref 'ConsoleHostedZone'
     Name: "resource-explorer.console.aws.amazon.com"
     AliasTarget:
       DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
       HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
     Type: A

 ConsoleRecordRegional:
   Type: AWS::Route53::RecordSet
   Properties:
     HostedZoneId: !Ref 'ConsoleHostedZone'
```

```
      Name: !Sub "${AWS::Region}.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  SigninHostedZone:
    Type: "AWS::Route53::HostedZone"
    Properties:
      HostedZoneConfig:
        Comment: 'Signin VPC Endpoint Hosted Zone'
      Name: 'signin.aws.amazon.com'
      VPCs:
        -
          VPCId: !Ref AppVPC
          VPCRegion: !Ref "AWS::Region"

  SigninRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'SigninHostedZone'
      Name: 'signin.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
      Type: A

  SigninRecordRegional:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'SigninHostedZone'
      Name: !Sub "${AWS::Region}.signin.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
      Type: A

##########################
```

```
# WORKSPACE RESOURCES
########################
  ADAdminSecret:
    Type: AWS::SecretsManager::Secret
    Properties:
      Name: "ADAdminSecret"
      Description: "Password for directory services admin"
      GenerateSecretString:
        SecretStringTemplate: '{"username": "Admin"}'
        GenerateStringKey: password
        PasswordLength: 30
        ExcludeCharacters: '"@/\'

  WorkspaceSimpleDirectory:
    Type: AWS::DirectoryService::SimpleAD
    DependsOn: AppVPC
    DependsOn: PrivateSubnetA
    DependsOn: PrivateSubnetB
    Properties:
      Name: "corp.awsconsole.com"
      Password: '{{resolve:secretsmanager:ADAdminSecret:SecretString:password}}'
      Size: "Small"
      VpcSettings:
        SubnetIds:
          - Ref: PrivateSubnetA
          - Ref: PrivateSubnetB

        VpcId:
          Ref: AppVPC


Outputs:
  PrivateSubnetA:
    Description: Private Subnet A
    Value: !Ref PrivateSubnetA

  PrivateSubnetB:
    Description: Private Subnet B
    Value: !Ref PrivateSubnetB

  WorkspaceSimpleDirectory:
    Description: Directory to be used for Workspaces
    Value: !Ref WorkspaceSimpleDirectory
```

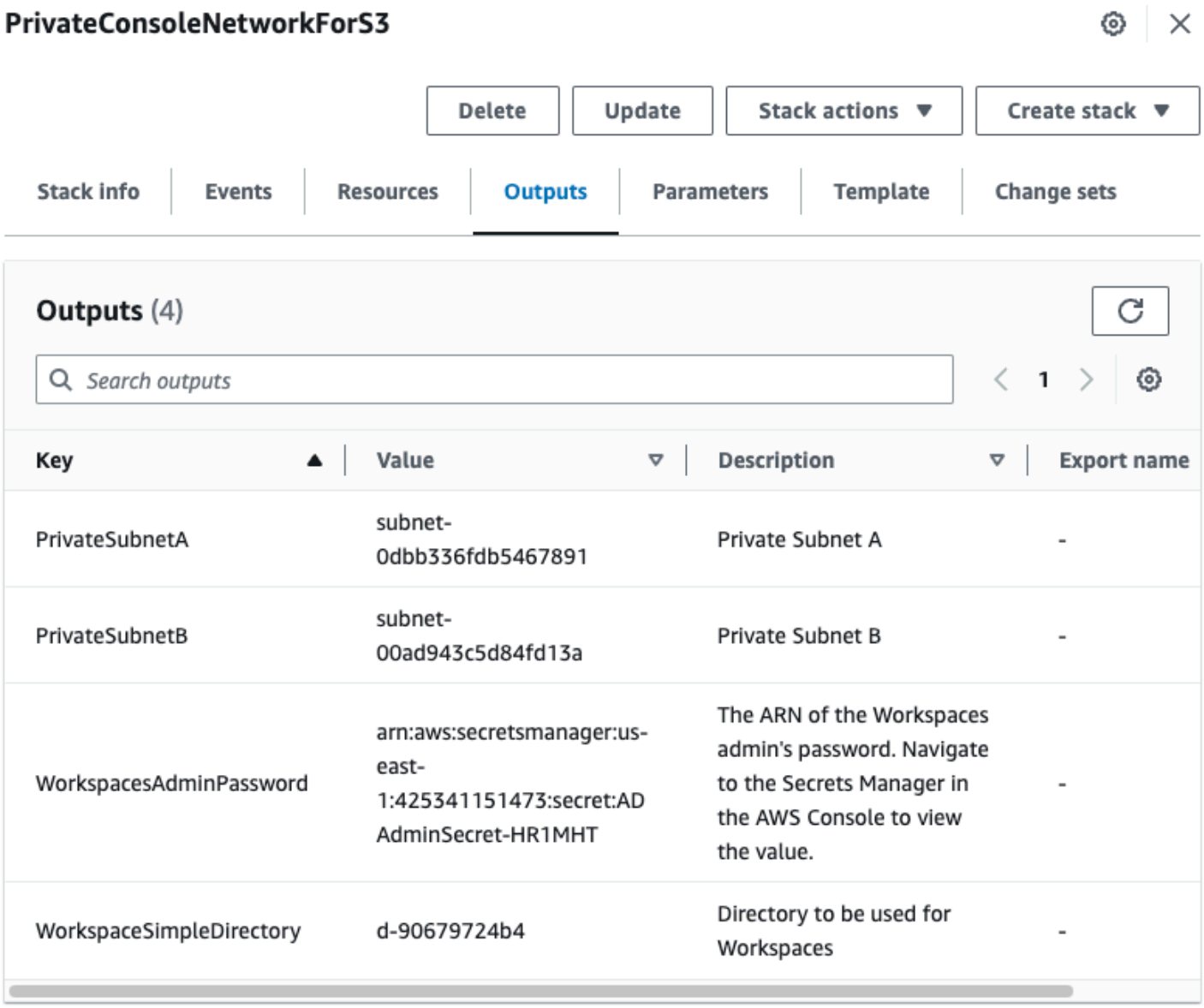
```
  WorkspacesAdminPassword:
    Description : "The ARN of the Workspaces admin's password.  Navigate to the Secrets
Manager in the AWS Console to view the value."
    Value: !Ref ADAdminSecret
```

> **Note**
>
> La configuración de esta prueba está diseñada para ejecutarse en la región Este de EE. UU. (Norte de Virginia) (us-east-1).

Para configurar una red

1. Inicie sesión en la cuenta de administración de su organización y abra la consola de AWS CloudFormation.
2. Seleccione Crear pila.
3. Elija With new resources (standard) (Con nuevos recursos [estándar]). Cargue el archivo de AWS CloudFormation plantilla que creó anteriormente y seleccione Siguiente.
4. Introduzca un nombre para la pila (por ejemplo, **`PrivateConsoleNetworkForS3`**) y, a continuación, seleccione Siguiente.
5. Para VPC y subredes, introduzca los rangos de CIDR de IP que prefiera o use los valores predeterminados proporcionados. Si utilizas los valores predeterminados, comprueba que no se superpongan con los recursos de VPC existentes en tu empresa. Cuenta de AWS
6. Seleccione Crear pila.
7. Una vez creada la pila, elija la pestaña Recursos para ver los recursos que se han creado.
8. Elija la pestaña Salidas para ver los valores de las subredes privadas y del Workspace Simple Directory. Toma nota de estos valores, ya que los utilizarás en el paso cuatro del siguiente procedimiento para crear y configurar un WorkSpace.

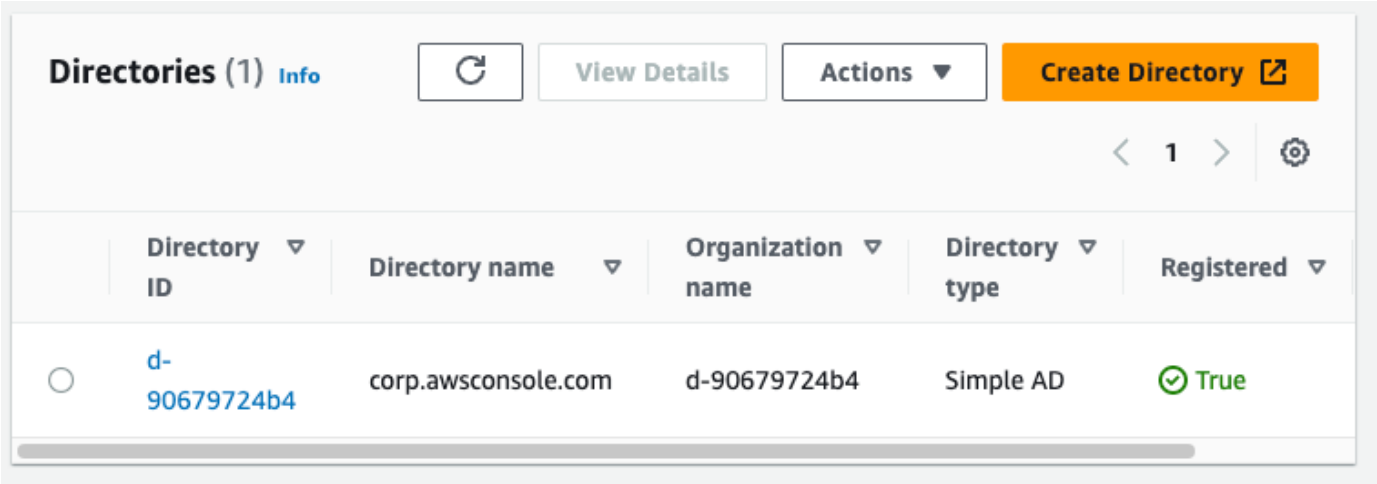
La siguiente captura de pantalla muestra la vista de la pestaña Salidas, que contiene los valores de las subredes privadas y del Workspace Simple Directory.



Ahora que ha creado su red, utilice los siguientes procedimientos para crear y acceder a WorkSpace.

Para crear un WorkSpace

1. Abra la consola de WorkSpaces .
2. En el panel de navegación, elija Directories (Directorios).
3. En la página Directorios, compruebe que el estado del directorio sea Activo. La siguiente captura de pantalla muestra una página Directorios con un directorio activo.



4. Para utilizar un directorio WorkSpaces, debe registrarlo. En el panel de navegación, elija y WorkSpaces, a continuación, elija Crear WorkSpaces.
5. En Seleccionar un directorio, elija el directorio creado por AWS CloudFormation en el procedimiento anterior. En el menú Acciones, seleccione Registrar.
6. Para la selección de subredes, seleccione las dos subredes privadas que se indican en el paso nueve del procedimiento anterior.
7. Seleccione Habilitar permisos de autoservicio y, a continuación, seleccione Registrar.
8. Una vez registrado el directorio, continúe con la creación del WorkSpace. Seleccione el directorio registrado y, a continuación, seleccione Siguiente.
9. En la página Crear usuarios, seleccione Crear usuario adicional. Introduzca su nombre y correo electrónico para poder utilizar el WorkSpace. Compruebe que la dirección de correo electrónico es válida, ya que la información de inicio de WorkSpace sesión se envía a esta dirección de correo electrónico.
10. Elija Siguiente.
11. En la página Identificar usuarios, seleccione el usuario que creó en el paso nueve y, a continuación, elija Siguiente.
12. En la página Seleccionar agrupación, elija Estándar con Amazon Linux 2 y, a continuación, seleccione Siguiente.
13. Utilice la configuración predeterminada para el modo de ejecución y la personalización del usuario y, a continuación, elija Crear Workspace. WorkSpace Comienza en `Pending` estado y pasa a ser `Available` de unos 20 minutos.
14. Cuando WorkSpace esté disponible, recibirás un correo electrónico con instrucciones para acceder a él en la dirección de correo electrónico que proporcionaste en el paso nueve.

Después de iniciar sesión en su WorkSpace cuenta, puede comprobar que está accediendo a ella con su acceso AWS Management Console privado.

Para acceder a un WorkSpace

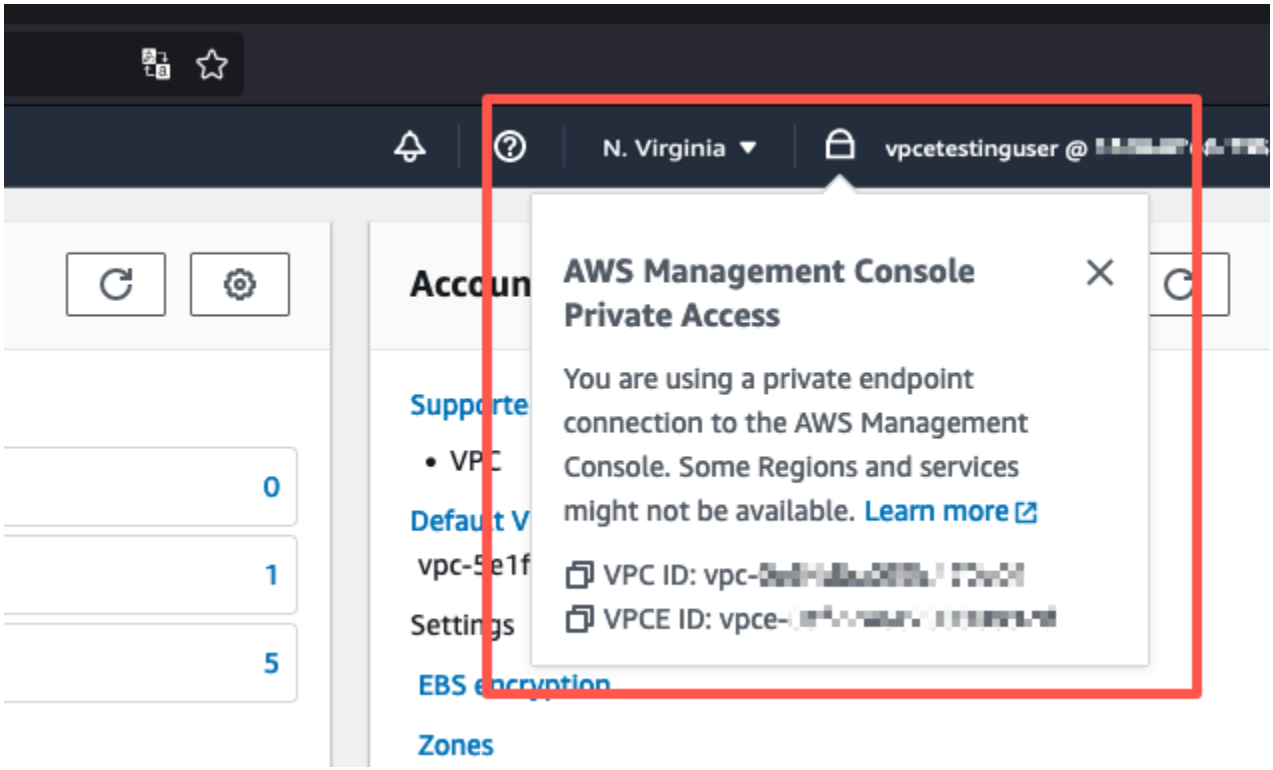
1. Abra el correo electrónico que recibió en el paso 14 del procedimiento anterior.
2. En el correo electrónico, elija el enlace exclusivo que se proporciona para configurar su perfil y descargar el WorkSpaces cliente.
3. Obtenga la contraseña
4. Descargue el cliente que desee.
5. Instale y ejecute el cliente. Introduzca el código de registro que se le ha enviado a su correo electrónico y, a continuación, seleccione Registrar.
6. Inicia sesión en Amazon WorkSpaces con las credenciales que creaste en el paso tres.

Para probar la configuración del acceso AWS Management Console privado

1. Desde tu WorkSpace, abre tu navegador. A continuación, navegue hasta AWS Management Console e inicie sesión con sus credenciales.

   > **Note**
   >
   > Si utiliza Firefox como navegador, compruebe que la opción Habilitar DNS a través de HTTPS esté desactivada en la configuración.

2. Abra la consola de Amazon S3, donde podrá comprobar que está conectado mediante AWS Management Console Private Access.
3. Elija el icono del candado en la barra de navegación para ver la VPC y el punto de conexión de VPC en uso. La siguiente captura de pantalla muestra la ubicación del icono del candado y la información de la VPC.



Pruebe la configuración de la VPC con políticas de IAM

Puede seguir probando la VPC que ha configurado con Amazon EC2 WorkSpaces o implementando políticas de IAM que restrinjan el acceso.

La siguiente política deniega el acceso a Amazon S3 a menos que utilice la VPC especificada.

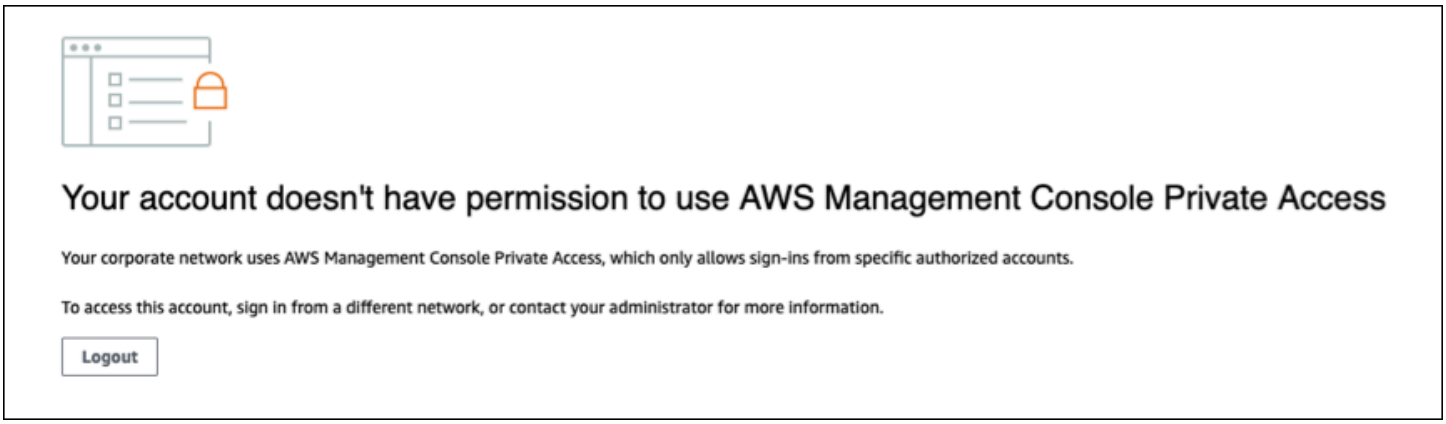
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "S3:*",
            "Resource": "*",
            "Condition": {
                "StringNotEqualsIfExists": {
                    "aws:SourceVpc": "sourceVPC"
                },
                "Bool": {
                    "aws:ViaAwsService": "false"
                }
            }
```

```
        }
    ]
}
```

La siguiente política limita el inicio de sesión a determinadas Cuenta de AWS ID mediante una política de acceso AWS Management Console privado para el punto final de inicio de sesión.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalAccount": [
                        "AWSAccountID"
                    ]
                }
            }
        }
    ]
}
```

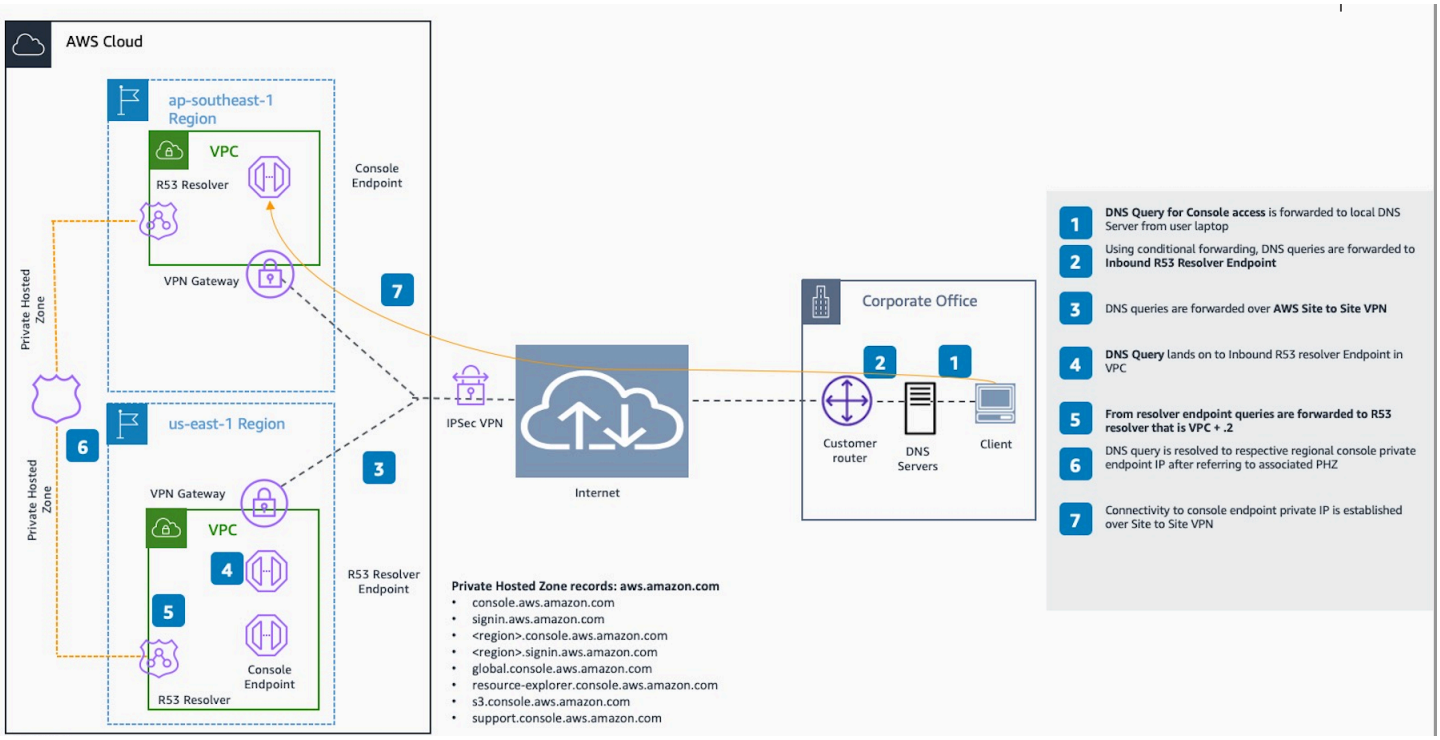
Si se conecta con una identidad que no pertenece a su cuenta, aparecerá la siguiente página de error.



Arquitectura de referencia

Para conectarte de forma AWS Management Console privada a Private Access desde una red local, puedes aprovechar la opción de conexión AWS Site-to-Site VPN a AWS Virtual Private Gateway (VGW). AWS Site-to-Site VPN permite el acceso a la red remota desde la VPC mediante la creación de una conexión y la configuración del enrutamiento para que el tráfico pase a través de la conexión. Para obtener más información, consulte Qué es la VPN de AWS sitio a sitio en la Guía del usuario de VPN de sitio a sitio.AWS AWS La puerta de enlace privada virtual (VGW) es un servicio regional de alta disponibilidad que actúa como puerta de enlace entre una VPC y la red local.

AWS Site-to-Site VPN a la puerta de enlace privada AWS virtual (VGW)



Un componente esencial de este diseño de arquitectura de referencia es el Amazon Route 53 Resolver resolutor entrante, específicamente. Al configurarlo en la VPC donde se crean los puntos de enlace de acceso AWS Management Console privado, los puntos de enlace de resolución (interfaces de red) se crean en las subredes especificadas. A continuación, se puede hacer referencia a las direcciones IP en los reenviadores condicionales de los servidores de DNS en las instalaciones para permitir la consulta de los registros de una zona alojada privada. Cuando los clientes locales se conectan a la AWS Management Console, se redirigen a las IP privadas de los puntos finales de acceso privado. AWS Management Console

Antes de configurar la conexión al punto final de acceso AWS Management Console privado, complete los pasos previos: configurar los puntos finales de acceso AWS Management Console privado en todas las regiones a las que desee acceder AWS Management Console, así como en la región de EE. UU. Este (Virginia del Norte), y configurar la zona alojada privada.

Lanzamiento de AWS CloudShell en la barra de herramientas de la consola

AWS CloudShell es un shell previamente autenticado y basado en el navegador, que se puede lanzar directamente desde la AWS CloudShell en la barra de herramientas de la consola. Puede ejecutar los comandos de la AWS CLI en los servicios utilizando el shell de su preferencia (Bash, PowerShell o Z shell).

Puede lanzar CloudShell desde la Console Toolbar utilizando uno de los dos métodos siguientes:

- Elija el icono de CloudShell en la esquina inferior izquierda de la consola.
- Elija el icono de CloudShell en la barra de navegación de la consola.

Para obtener más información sobre este servicio, consulte la Guía del usuario de AWS CloudShell.

Para obtener información sobre las Regiones de AWS en las que está disponible Regiones de AWS, consulte la Lista de servicios regionales de AWS. La selección de la región de la consola está sincronizada con la región de CloudShell. Si CloudShell no está disponible en una región seleccionada, funcionará en la región más cercana.

Obtención de información de facturación

Si dispone de los permisos necesarios, puede obtener información sobre sus cargos de AWS en la consola.

Para obtener la información de facturación

1. En la barra de navegación, elija el nombre de la cuenta.
2. Elija My Billing Dashboard (Mi panel de facturación).
3. Utilice el panel AWS Billing and Cost Management para buscar un resumen y un desglose de su gasto mensual. Para obtener más información, consulte la AWS Billing Guía del usuario.

Uso de Markdown en la consola

Algunos servicios de AWS Management Console, como Amazon CloudWatch, admiten el uso de Markdown en determinados campos. En este tema se explican los tipos de formato de Markdown admitidos en la consola.

Contenido

Párrafos, espaciado de líneas y líneas horizontales

Los párrafos se separan mediante una línea en blanco. Para asegurarse de que se reproduce la línea en blanco entre los párrafos cuando se convierta a HTML, agregue una nueva línea con un espacio sin salto (` `) y, a continuación, una línea en blanco. Repita este par de líneas para insertar varias líneas en blanco sucesivamente, como en el siguiente ejemplo:

```
 

 
```

Para crear una regla horizontal que separe los párrafos, agregue una nueva línea con tres guiones seguidos: `---`

```
Previous paragraph.
---
Next paragraph.
```

Para crear un bloque de texto con tipo monoespaciado, agregue una línea con tres puntos suspensivos (`). Ingrese el texto que desea mostrar en tipo monoespaciado. A continuación, agregue

otra línea nueva con tres marcas de retroceso. En el siguiente ejemplo se muestra un texto al que se le dará formato de tipo monoespaciado cuando se muestre:

```
```
This appears in a text box with a background shading.
The text is in monospace.
```
```

Encabezados

Para crear títulos, utilice la almohadilla (#). Una sola almohadilla y un espacio indican un título de nivel superior. Dos almohadillas crean un título de segundo nivel y tres almohadillas crean un título de tercer nivel. En los siguientes ejemplos se muestra un título de primer nivel, de segundo nivel y de tercer nivel:

```
# Top-level heading
```

```
## Second-level heading
```

```
### Third-level heading
```

Formato de texto

Para poner texto en cursiva, incluya un carácter de subrayado (_) o un asterisco (*) a cada lado.

```
*This text appears in italics.*
```

Para poner texto en negrita, incluya dos caracteres de subrayado o dos asteriscos a cada lado.

```
**This text appears in bold.**
```

Para tachar texto, incluya dos tildes (~) a cada lado.

```
~~This text appears in strikethrough.~~
```

Enlaces

Para agregar un hiperenlace de texto, ingrese el texto del enlace entre corchetes ([ ]), seguido de la URL completa entre paréntesis (( )), como en el siguiente ejemplo:

```
Choose [link_text](http://my.example.com).
```

Lists

Para dar formato a las líneas como parte de una lista con viñetas, agréguelas en líneas separadas que comiencen por un solo asterisco (*) y, después, un espacio, como en el siguiente ejemplo:

```
Here is a bulleted list:
* Ant
* Bug
* Caterpillar
```

Para dar formato a las líneas como parte de una lista numerada, agréguelas en líneas separadas que comiencen por un número, un punto (.) y un espacio, como en el siguiente ejemplo:

```
Here is a numbered list:
1. Do the first step
2. Do the next step
3. Do the final step
```

Tablas y botones (CloudWatch paneles de control)

CloudWatch Los widgets de texto de los paneles admiten tablas y botones de Markdown.

Para crear una tabla, separe las columnas con barras verticales (|) y las filas con saltos de línea. Para que la primera fila sea de título, inserte una línea entre la fila de título y la primera fila de valores. A continuación, agregue al menos tres guiones (-) para cada columna de la tabla. Separe las columnas con barras verticales. En el siguiente ejemplo se muestra el formato Markdown para una tabla con dos columnas, una fila de título y dos filas de datos:

```
Table | Header
----|-----
Amazon Web Services | AWS
```

```
1 | 2
```

El texto en formato Markdown del ejemplo anterior crea la siguiente tabla:

Tabla	Encabezado
Amazon Web Services	AWS
1	2

En un widget de texto de CloudWatch panel, también puedes formatear un hipervínculo para que aparezca como un botón. Para crear un botón, utilice `[button:`*`Button text`*`]`, seguido de la URL completa entre paréntesis(( )), como en el siguiente ejemplo:

```
[button:Go to AWS](http://my.example.com)
[button:primary:This button stands out even more](http://my.example.com)
```

Resolución de problemas

Consulte esta sección para encontrar soluciones a problemas comunes con el AWS Management Console.

También puedes diagnosticar y solucionar errores comunes de algunos AWS servicios mediante Amazon Q Developer. Para obtener más información, consulte Diagnosticar errores comunes en la consola con Amazon Q Developer en la Guía del usuario de Amazon Q Developer.

Temas

La página no se está cargando correctamente

- Si este problema solo se produce de vez en cuando, compruebe su conexión a Internet. Intente conectarse a través de una red diferente, o con o sin una VPN, o intente usar un navegador web diferente.
- Si todos los usuarios afectados pertenecen al mismo equipo, es posible que se trate de un problema de privacidad, de una extensión del navegador o de un firewall de seguridad. Las extensiones de privacidad del navegador y los firewalls de seguridad pueden bloquear el acceso a los dominios utilizados por el AWS Management Console. Pruebe a desactivar estas extensiones o a ajustar la configuración del firewall. Para comprobar los problemas con la conexión, abra las herramientas para desarrolladores del navegador (Chrome,Firefox) e inspeccione los errores en la pestaña Console (Consola). AWS Management Console Utiliza los sufijos de los dominios, incluida la siguiente lista. Esta lista no es exhaustiva y puede cambiar con el tiempo. AWS no utiliza de forma exclusiva los sufijos de estos dominios.
  - .a2z.com
  - amazon.com
  - .amazonaws.com

- .aws
- .aws.com
- .aws.dev
- .awscloud.com
- .awsplayer.com
- .awsstatic.com
- *.cloudfront.net
- .live-video.net

> **Warning**
>
> Desde el 31 de julio de 2022, ya AWS no es compatible con Internet Explorer 11. Le recomendamos que lo utilice AWS Management Console con otros navegadores compatibles. Para obtener más información, consulte AWS News Blog.

Mi navegador muestra un error de «acceso denegado» al conectarme al AWS Management Console

Los cambios recientes realizados en la consola pueden afectar a tu acceso si utilizas todo lo siguiente:

- Un navegador desde una VPC.
- Puntos finales de VPC.
- Políticas de IAM que contienen una clave de condición `aws:SourceIp` global.

En la consola, vaya a la página de políticas de IAM. Le recomendamos que revise las políticas de IAM que contienen una clave de condición `aws:SourceIp` global y que añada `aws:SourceVpc` una clave.

Como alternativa, puede considerar la posibilidad de incorporar la función de acceso AWS Management Console privado para acceder a ella a AWS Management Console través de un punto final de VPC y `aws:SourceVpc` utilizar las condiciones de sus políticas. Para obtener más información, consulte AWS Management Console Acceso privado.

Mi navegador muestra errores de tiempo de espera al conectarme al AWS Management Console

Si hay una interrupción del servicio en tu configuración predeterminada Región de AWS, es posible que tu navegador muestre un error de tiempo de espera 504 Gateway al intentar conectarse al. AWS Management Console Para iniciar sesión AWS Management Console desde una región diferente, especifica un punto final regional alternativo en la URL. Por ejemplo, si hay una interrupción en la región `us-west-1` (N. California), para acceder a la región `us-west-2` (Oregón) utilice la siguiente plantilla:

```
https://region-code.console.aws.amazon.com
```

Para obtener más información, consulte Puntos de conexión del servicio de la AWS Management Console en la Referencia general de AWS.

Para ver el estado de todos Servicios de AWS, incluido el AWS Management Console, consulte AWS Health Dashboard.

Quiero cambiar el idioma de AWS Management Console pero no encuentro el menú de selección de idioma en la parte inferior de la página

El menú de selección de idioma se ha movido a la nueva página de configuración unificada. Para cambiar el idioma de la consola AWS Management Console, vaya a la página de configuración unificada y, a continuación, elija el idioma de la consola.

Para obtener más información, consulte Cambio del idioma de la AWS Management Console.

Historial de documentos

En la siguiente tabla se describen cambios importantes en la Guía de introducción de AWS Management Console , a partir de marzo de 2021.

Cambio	Descripción	Fecha
Chatea con Amazon Q	Una nueva página de configuración que detalla cómo los usuarios pueden hacer AWS preguntas al desarrollador de Amazon Q. Para obtener más información, consulte Chat con un desarrollador de Amazon Q.	29 de mayo de 2024
Mis aplicaciones	Una nueva página que presenta MyApplications. Para obtener más información, consulte ¿En qué consiste MyApplications? AWS .	29 de noviembre de 2023
Establecimiento de la configuración unificada	Una nueva página de configuración para establecer las opciones y los valores predeterminados que se aplican al usuario actual, incluidos el idioma y la región. Para obtener más información, consulte Establecimiento de la configuración unificada.	6 de abril de 2022
Nueva AWS Console Home interfaz de usuario	Nueva AWS Console Home interfaz de usuario, que incluye widgets para mostrar información de uso importante y accesos directos a los AWS	25 de febrero de 2022

Cambio	Descripción	Fecha
	servicios. Para obtener más información, consulte Trabajar con widgets.	
Cambio del idioma de la consola	Elija otro idioma para la AWS Management Console. Para obtener más información, consulte Cambio del idioma de la AWS Management Console.	1 de abril de 2021
Lanzamiento CloudShell	Abra AWS CloudShell desde AWS Management Console y ejecute los comandos AWS CLI. Para obtener más información, consulte Lanzamiento AWS CloudShell.	22 de marzo de 2021

Glosario de AWS

Para ver la terminología más reciente de AWS, consulte el Glosario de AWS en la Referencia de Glosario de AWS.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.